ViPNet SafeDisk-V 4.2

Benutzerhandbuch



Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Copyright

Version: 00077-02 34 01 DEU

Marken

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

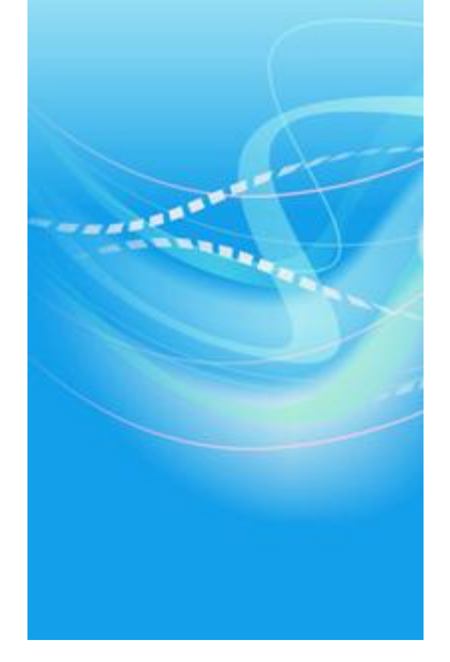
Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.biz

Inhalt



Einführung

Über dieses Dokument

Zielgruppe

Dieses Handbuch ist für alle bestimmt, die das Programm ViPNet SafeDisk-V für den schnellen, einfachen und effektiven Schutz von Daten einsetzen wollen.

Zu Beginn des Handbuchs werden die allgemeinen Grundlagen der Technologie von ViPNet SafeDisk-V erklärt. Anschließend wird der Vorgang der Installation von ViPNet SafeDisk-V beschrieben. In den nachfolgenden Kapiteln erfahren Sie mehr über die Aufgaben, die mit Hilfe von ViPNet SafeDisk-V gelöst werden können. Am Ende wird eine kurze Übersicht von Anleitungen zur Suche und Beseitigung von Störungen geboten, womit einige häufig auftretende Probleme schnell beseitigt werden können.

Das in diesem Handbuch vorgestellte Material ist nach steigendem Schwierigkeitsgrad angeordnet. Nach dem Erhalt der notwendigen Informationen können Sie mit dem Lesen aufhören und zum Handbuch wieder zurückkehren, wenn dazu die Notwendigkeit besteht.

Die Kapitel können auch in beliebiger Reihenfolge gelesen werden. Sie finden die benötigten Informationen bequem mit Hilfe der Inhaltsübersicht und des Stichwortverzeichnisses.

Beim Verfassen dieses Handbuchs sind wir davon ausgegangen, dass der Leser über Basiskenntnisse über das Betriebssystem Windows verfügt und sich über die Notwendigkeit des Schutzes vertraulicher Daten im Klaren ist.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
⚠	**Achtung!** Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
ℹ	**Hinweis.** Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.

Symbol	Beschreibung
💡	**Tipp.** Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Über dieses Programm

Gegenwärtig steigt der Wert vertrauenswürdiger Information stetig an, und der Verlust von Daten kann schwerwiegende Folgen nach sich ziehen.

Etwaige Übeltäter oder nicht berechtigte Personen könnten Interesse daran haben, auf unterschiedliche Daten Ihrer Firma wie Geschäftsdatenverkehr, Berichte über die Aktivitäten des Unternehmens, innovative Ideen und Entwicklungen u. s. w. zuzugreifen. Die Ziele könnten der Erhalt materieller Entschädigungen, das Verursachen von Imageschäden oder der Diebstahl geistigen Eigentums sein.

Folglich sollten Ihre Daten unbedingt vor unberechtigtem Lesen, Kopieren, Ändern oder Löschen durch Unbefugte geschützt werden. Ganz besonders müssen Sie auf den Schutz Ihrer Daten achten, wenn Sie Notebooks benutzen, da diese leicht ohne Aufsicht bleiben oder gestohlen werden können. Daneben muss ein effektiver Zugriff auf geschützte Daten für Personen, die diese zum Arbeiten benötigen (zum Beispiel Ihre Mitarbeiter) sichergestellt werden.

Der Schutz von Daten sollte aber nicht zu viel Zeit und Mühe in Anspruch nehmen und keine Kenntnisse in Kryptographie voraussetzen. Die Vorgänge zur Ver- und Entschlüsselung sollten transparent ablaufen und keine aktive Teilnahme des Benutzers erfordern. Außerdem sollte die verwendete Software vollständig in die bestehenden Geschäftsprozesse der Firma sowie in bereits implementierte Lösungen im Bereich der Informationssicherheit integriert sein.

Die vorliegende Version des Programms ViPNet SafeDisk-V, die einen Bestandteil der Lösungen ViPNet CUSTOM und ViPNet VPN bildet, erfüllt alle aufgezählten Anforderungen.

Systemanforderungen



Hinweis. Die Anforderungen an den Computer für die Installation von ViPNet SafeDisk-V sind mit den Anforderungen für die Installation von ViPNet Client identisch.

Folgende Mindestanforderungen müssen vom Computer für den Einsatz von ViPNet SafeDisk-V erfüllt werden:

- Intel Core 2 Duo E6400 oder andere x86-kompatible Prozessoren mit zwei Kernen oder mehr werden empfohlen.

- Mindestens 512 MB RAM, 1 GB ist empfohlen.
- Mindestens 150 MB freier Speicherplatz, empfohlen sind 250 MB.
- Betriebssysteme: Windows XP SP3 (32-Bit), Server 2003 (32-Bit), Vista SP2 (32/64-Bit), Server 2008 (32/64-Bit), Windows 7 (32/64-Bit), Server 2008 R2 (64-Bit).
- Internet Explorer 6.0 oder höher.

Anforderungen an die Softwareumgebung

Für den korrekten Betrieb dieser Version von ViPNet SafeDisk-V müssen folgende Bedingungen erfüllt sein:

- Auf dem Computer muss die Software ViPNet Client oder ViPNet Coordinator Version nicht niedriger als 4.0.x installiert sein.
- Auf dem Netzwerkknoten (s. ViPNet Netzwerkknoten auf S. 146) muss die Schlüsseldistribution (auf S. 145) eines ViPNet Benutzers installiert sein.
- Der Netzwerknoten sollte in der Rolle „Safe Disk“ (s. Rolle auf S. 145) im ViPNet Network Control Center (s. Network Control Center (NCC) auf S. 144) registriert sein, oder dem gegebenen Netzwerkknoten sollte im Programm ViPNet Network Manager (auf S. 145) die Arbeit mit dem Programm ViPNet SafeDisk-V erlaubt werden.
- Die Lizenz für das ViPNet Netzwerk darf nicht abgelaufen sein.
- Auf dem Computer muss die Software ViPNet Client Monitor oder ViPNet Coordinator Monitor gestartet sein.
- Die Software ViPNet Client Monitor oder ViPNet Coordinator Monitor sollte sich nicht in einer Konfiguration befinden, die für die Arbeit mit Containern nicht zulässig ist („Offenes Internet“, „Internet“).



Hinweis. Die Installation von ViPNet SafeDisk-V auf dem Computer kann auch unabhängig von der Erfüllung der weiter oben aufgezählten Bedingungen vorgenommen werden. Wenn jedoch zumindest eine der Bedingungen nicht erfüllt ist, wird der Start des Programms nicht möglich sein.

Lieferumfang

Zum Lieferumfang von ViPNet SafeDisk-V gehören:

- Installationsdatei;

- „ViPNet SafeDisk-V. Benutzerhandbuch“.

Die Dokumentation wird in elektronischer Form geliefert.

Neue Möglichkeiten der Version 4.2

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten von ViPNet SafeDisk-V der Version 4.2 geboten.

- **Integration mit dem Programm ViPNet Coordinator**

  Zuvor war das Programm ViPNet SafeDisk-V lediglich mit dem Programm ViPNet Client integriert. Nun wird zusätzlich die Integration von ViPNet SafeDisk-V mit dem Programm ViPNet Coordinator unterstützt.

- **Änderungen im Interaktionsprinzip zwischen ViPNet SafeDisk-V und ViPNet Monitor**

  Beim Arbeiten mit geschützten Containern sollten nun Trafficschutz-Parameter konfiguriert werden, die anschließend vom Programm ViPNet Monitor übernommen werden. Dies gewährleistet den zusätzlichen Schutz vor unbefugten Zugriffen auf geschützte Container seitens der Benutzer sowohl des offenen als auch des privaten Netzwerks (zum Beispiel können bei einer bestimmten Konfiguration der Trafficschutz-Parameter weder der Netzwerkadministrator noch der ViPNet Netzwerkadministrator einen Zugang zu geschützten Containern erhalten).

- **Zwangsweises Beenden aller Anwendung und Abmeldung in Windows, wenn das Trennen der Container im Modus „Gefahr“ oder „Extreme Gefahr“ nicht möglich ist**

  Wenn SafeDisk-V in früheren Versionen die Container nicht sofort trennen konnte, wurde die Schließung aller Anwendungen und die Abmeldung unter Windows innerhalb von 60 Sekunden durchgeführt. Nun werden die Schließung der Anwendungen und die Abmeldung der Windows-Sitzung beim Trennen der Container im Modus „Gefahr“ und „Extreme Gefahr“ unverzüglich durchgeführt.

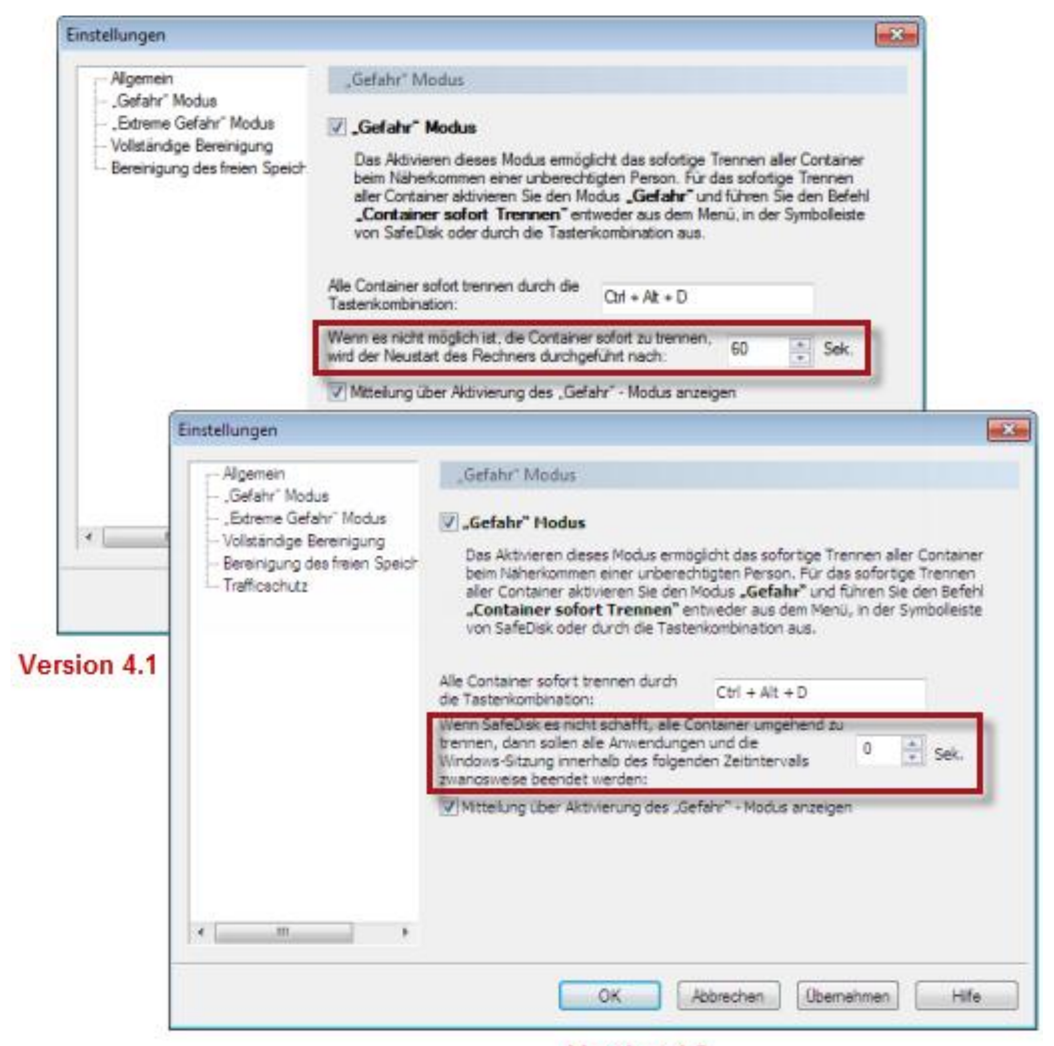


Abbildung 1: Sofortiges Trennen der Container

- **Neues Installationsprogramm von ViPNet SafeDisk-V**

  Für ViPNet SafeDisk-V der Version 4.2 wurde ein neues Installationsprogramm entwickelt, in welchem die MSI-Technologie verwendet wird.

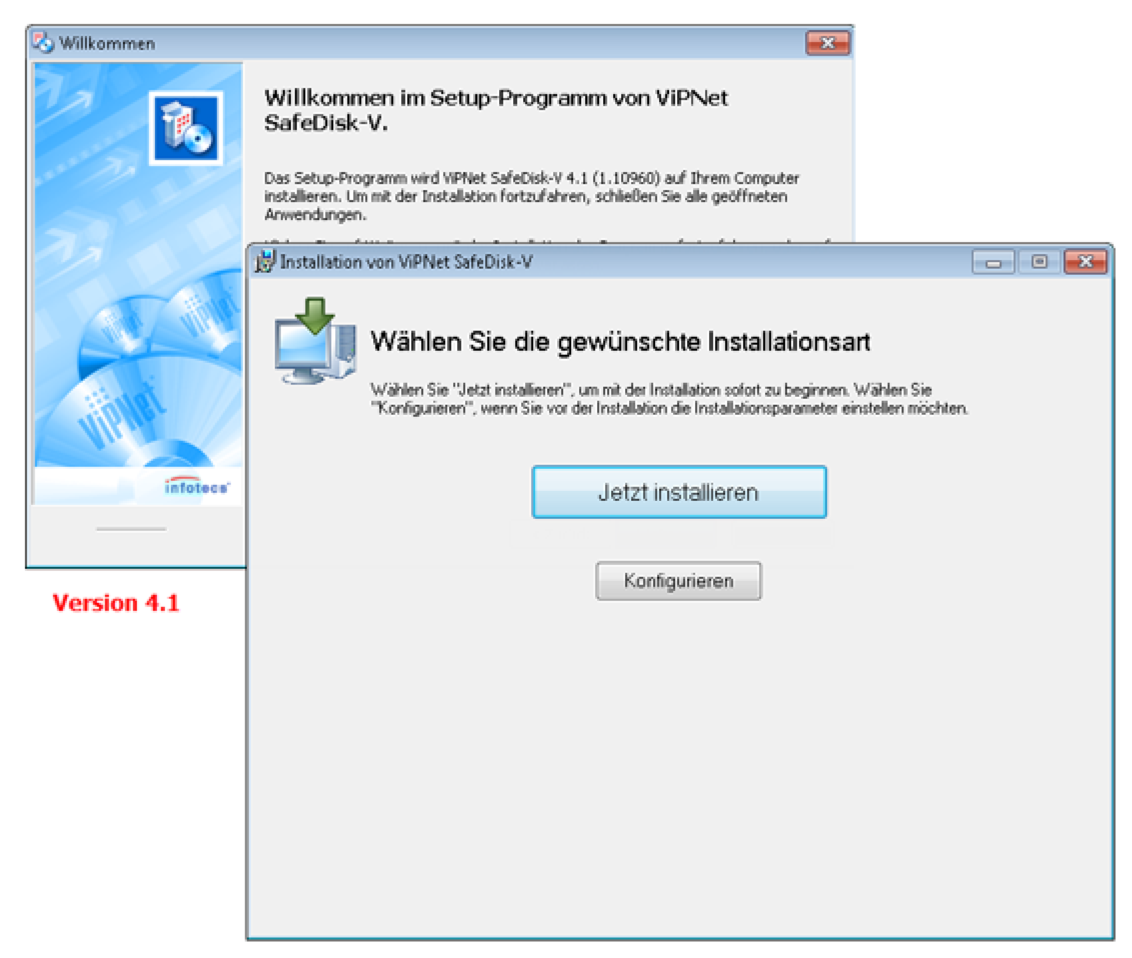


Abbildung 2: Neues Installationsprogramm

Kontakt

FAQ und andere Hilfsinformation

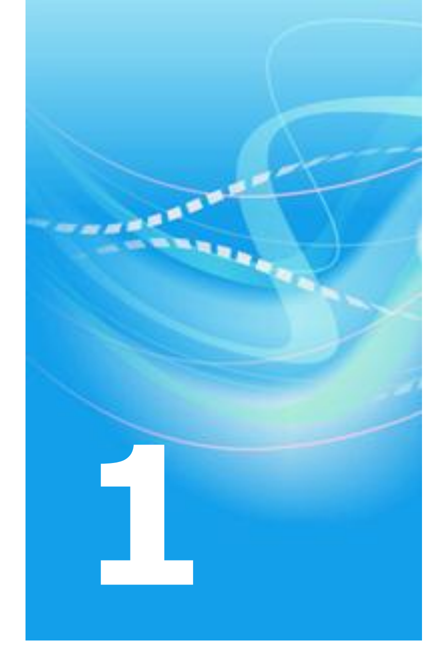
Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Fachleuten der Firma „InfoTeCS“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.biz.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 0 (Tel.); +49 (0) 30 206 43 66 66 (Fax).



Allgemeines

Einsatzmöglichkeiten von ViPNet SafeDisk-V

ViPNet SafeDisk-V hilft Ihnen dabei, folgende Aufgaben schnell und effektiv zu lösen:

- Sie wollen sicher sein, dass Ihre Verwandten, Freunde und Kollegen nicht die Möglichkeit haben, absichtlich oder durch Zufall, wichtige Dokumente einzusehen, zu ändern oder zu löschen;
- Sie speichern Daten auf einem Notebook und wollen nicht, dass diese von irgendjemandem sonst gelesen, kopiert oder benutzt werden (falls das Notebook verloren oder gestohlen wird);
- vertrauliche Daten werden auf mehreren Computern aufbewahrt (zum Beispiel zu Hause und im Büro) und Sie wollen die Rechner so schützen, dass ein sicherer Datenaustausch zwischen den Computern möglich wird;
- Sie wollen vertrauliche Daten mit Hilfe eines externen Datenträgers übertragen und gleichzeitig verhindern, dass die Daten verloren gehen oder gestohlen werden;
- Sie wollen den Zugang zu vertraulichen Daten auf einem oder mehreren Computern steuern können (zum Beispiel den Zugang zu Dokumenten für einige Benutzer erlauben und für andere Benutzer blockieren);
- bei der Annäherung Dritter wollen Sie den Zugang zu sensiblen Daten sperren und die Präsenz dieser Daten verbergen können;
- bei der Annäherung von Übeltätern wollen Sie alle vertraulichen Daten schnell und sicher löschen können.

Die Grundsätze des Datenschutzes in ViPNet SafeDisk-V: ein Überblick

In ViPNet SafeDisk-V wird ein Container erstellt, der in Form einer verschlüsselten Datei auf der Festplatte oder auf einem abnehmbaren Datenträger gespeichert wird.

Nach dem Einbinden wird der Container im System als ein gewöhnliches Laufwerk dargestellt, auf welchem vertrauliche Informationen abgelegt werden können.

Beim Speichern werden die Daten automatisch verschlüsselt und beim Auslesen automatisch entschlüsselt. Die Verschlüsselung erfolgt schnell und unauffällig, mit den Dokumenten kann wie im Normalbetrieb weitergearbeitet werden, die Daten werden dabei aber zuverlässig geschützt.

Die Ver- und Entschlüsselung der Daten erfolgt sektorweise beim Speichern und Lesen. Dementsprechend wird der Vorgang der Ver- oder Entschlüsselung nur für die Daten vollzogen, die zum aktuellen Zeitpunkt unmittelbar gebraucht werden. Das gewährleistet eine hohe Geschwindigkeit bei der Arbeit mit geschützten Daten und eine hohe Transparenz für die Benutzer der Anwendung.

Wenn sich der Container auf einem Netzlaufwerk befindet, werden die Daten verschlüsselt über das Netzwerk übertragen; die Ver- und Entschlüsselung erfolgt auf dem lokalen Rechner.

Nach dem Trennen wird der Container nicht mehr im System angezeigt. Die Präsenz vertraulicher Daten kann nicht mehr festgestellt werden, der Zugang zu diesen Daten ist nicht mehr möglich.

Zum Wiederherstellen des Zugangs zu den im Container abgelegten Daten und zum Fortsetzen der Arbeit mit diesen Daten muss der Container wieder eingebunden werden.

Zusammenarbeit im Programm ViPNet Client und ViPNet Coordinator

Die vorliegende Version des Programms ViPNet SafeDisk-V ist in der Softwarelösungen ViPNet CUSTOM und ViPNet VPN integriert und kann zusammen mit den Programmen ViPNet Client und ViPNet Coordinator verwendet werden.

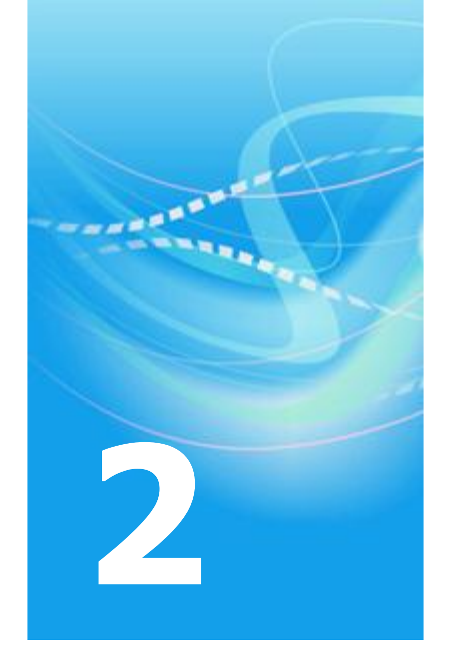


Achtung! Die Software ViPNet SafeDisk-V Version 4.2 kann nur gemeinsam mit der Software ViPNet Client und ViPNet Coordinator der Version 4.x oder höher verwendet werden.

Diese Art der Integration ermöglicht eine strenge Abgrenzung des Benutzerzugangs zu vertraulichen Daten, die sich in SafeDisk-V-Containern befinden: das Programm kann nur von einem Benutzer gestartet werden, der auf dem gegebenen ViPNet Netzwerkknoten registriert ist.

Auf diese Weise ermöglicht es die Integration von ViPNet SafeDisk-V mit dem Programm ViPNet Monitor dem Administrator des ViPNet Netzwerks, die Anwendung der unternehmensinternen Sicherheitsrichtlinie zentralisiert durchzusetzen. Zum Beispiel ist in den Konfigurationen des Programms ViPNet Monitor, die für die Arbeit im Internet bestimmt sind („Offenes Internet", „Internet"), das Arbeiten mit ViPNet SafeDisk verboten, wodurch das Risiko des Verlusts vertraulicher Daten verringert wird.

Ausführliche Informationen zur Verwendung von Konfigurationen des Programms ViPNet Monitor sind im Dokument „ViPNet Client Monitor. Benutzerhandbuch" bzw. „ViPNet Coordinator Monitor. Administratorhandbuch" enthalten.



Installation und Start von ViPNet SafeDisk-V

ViPNet SafeDisk-V installieren



Achtung! Wenn das Programm ViPNet SafeDisk-V auf einem Computer mit dem Betriebssystem Windows installiert wird, dessen Lokalisierung nicht Deutsch ist, müssen für die korrekte Darstellung von Umlauten auf der Benutzeroberfläche von ViPNet SafeDisk-V die regionalen Einstellungen von Windows entsprechend angepasst werden (s. Regionaleinstellungen auf S. 134).

Für die ordnungsgemäße Installation von ViPNet SafeDisk-V muss der Benutzer über Administratorrechte verfügen.

Zum Installieren des Programms gehen Sie folgendermaßen vor:

1. Starten Sie die Datei `setup.exe` und folgen Sie den Anweisungen des Installationsassistenten.
2. Machen Sie sich mit den Bedingungen der Lizenzvereinbarung vertraut. Falls Sie einverstanden sind, aktivieren Sie das entsprechende Kontrollkästchen. Klicken Sie dann auf **Fortsetzen**.
3. Wenn Sie die Installationsparameter einstellen möchten, dann klicken Sie auf **Konfigurieren** und definieren Sie die Werte für die folgenden Elemente:
   - Komponenten von ViPNet SafeDisk-V, die installiert werden sollen;
   - Pfad zum Installationsordner der ViPNet SafeDisk-V-Komponenten auf dem Computer;
   - Benutzername und Name der Organisation;
   - Ordnername für das Programm ViPNet SafeDisk-V im Menü Start.

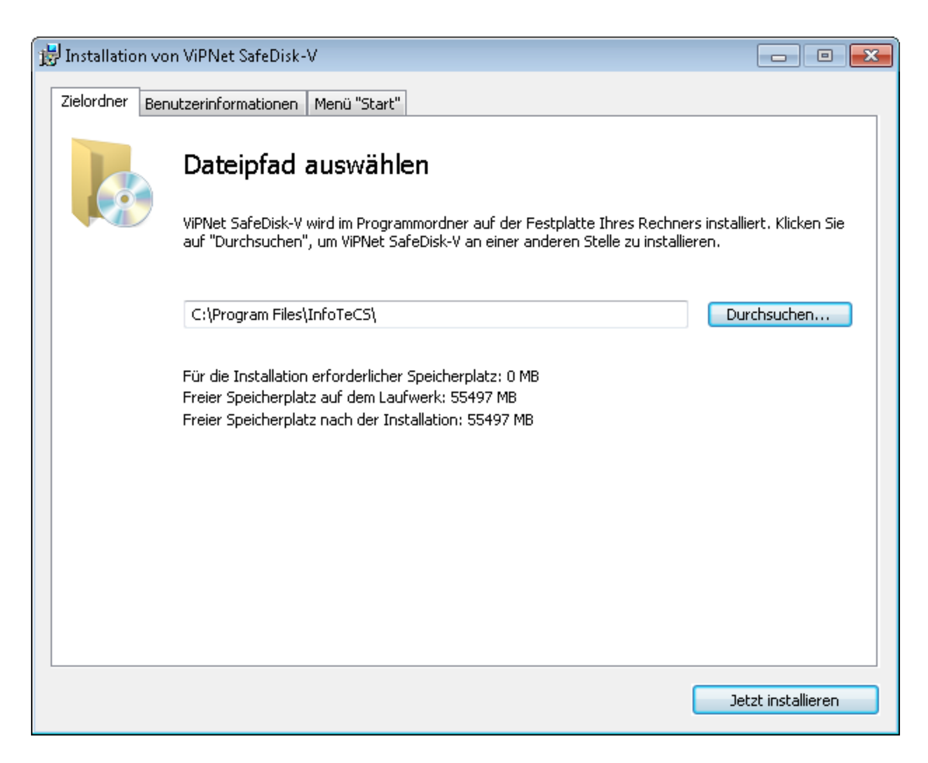


Abbildung 3: Konfiguration von Installationsparameter

4. Klicken Sie auf die Schaltfläche **Jetzt installieren**, um die Installation von ViPNet SafeDisk-V zu beginnen.
5. Wenn nach der Fertigstellung der Installation eine Meldung eingeblendet wird, dass der Computer neu gestartet werden soll, dann führen Sie einen Neustart des Computers durch.

Das Programm ViPNet SafeDisk-V ist nun installiert.

ViPNet SafeDisk-V starten



Achtung! Für das Ausführen von ViPNet SafeDisk-V ist es erforderlich, dass das Programm ViPNet Monitor gestartet ist. Wenn das Programm ViPNet Monitor nicht gestartet oder in der Konfiguration „Internet“ oder „Offenes Internet“ gestartet ist, dann wird eine entsprechende Meldung angezeigt und das Ausführen von ViPNet SafeDisk-V wird nicht möglich sein.

Das Programm ViPNet SafeDisk-V kann ausschließlich auf Netzwerkknoten mit der Rolle „SafeDisk“ verwendet werden. Wenn diese Rolle einem Knoten nicht zugewiesen ist, dann kann das Programm dort nicht gestartet werden.

Zum Starten von ViPNet SafeDisk-V:

1 Führen Sie eine der Aktionen aus:

- Wählen Sie im Menü **Start** den Eintrag **Alle Programme** > **ViPNet** > **ViPNet SafeDisk** und klicken Sie auf **ViPNet SafeDisk** (im Zuge der Installation könnte sich die Position des Programmeintrags im Menü **Start** auch geändert haben)
- Doppelklicken Sie auf dem Desktop auf die Verknüpfung (die Verknüpfung wird auf dem Desktop angezeigt, wenn im Zuge der Programminstallation eine entsprechende Option gewählt wurde).

Es wird das Anmeldefenster für das Programm ViPNet SafeDisk-V eingeblendet.

2 Geben Sie im Fenster **ViPNet SafeDisk-V** den Arbeitsmodus im offenen und privaten Netzwerk während der Verwendung der geschützten Container an (s. Konfiguration der Parameter für die Trafficblockierung bei Verwendung geschützter Container auf S. 60).

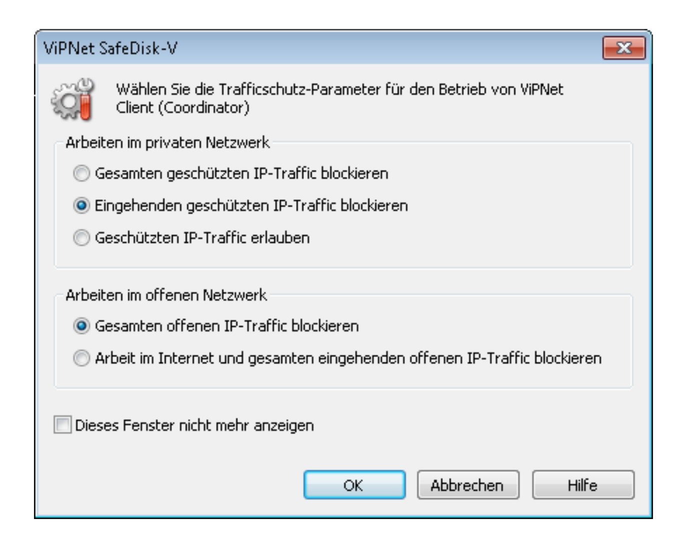


Abbildung 4: Konfiguration der Trafficschutz-Parameter für ViPNet SafeDisk-V

Wenn Sie den Arbeitsmodus für das offene und private Netzwerk nicht bei jedem Start von ViPNet SafeDisk-V einstellen möchten, dann aktivieren Sie das Kontrollkästchen **Dieses Fenster nicht mehr anzeigen**. Bei Bedarf können diese Parameter während der Arbeit mit ViPNet SafeDisk geändert werden (s. Konfiguration der Parameter für die Trafficblockierung bei Verwendung geschützter Container auf S. 60).

Als Ergebnis wird ViPNet SafeDisk-V gestartet. Wenn bereits Container existieren, für welche die automatische Einbindung beim Start von ViPNet SafeDisk-V eingestellt ist, und wenn in der aktuellen Konfiguration von ViPNet Monitor die Verwendung der Container erlaubt ist, werden diese Container nun eingebunden.

Nach dem Start von ViPNet SafeDisk-V werden die in ViPNet SafeDisk-V eingestellten Trafficschutz-Parameter im Programm ViPNet Monitor angewendet und die Benutzeroberfläche des Programms ViPNet Monitor wird eingeschränkt. Details zur gemeinsamen Nutzung von ViPNet Monitor und ViPNet SafeDisk-V s. Abschnitt „Integration mit ViPNet SafeDisk-V“ im Dokument „ViPNet Client Monitor. Benutzerhandbuch“ bzw. „ViPNet Coordinator Monitor. Administratorhandbuch“.

ViPNet SafeDisk-V beenden



Achtung! Für den erfolgreichen Start von ViPNet SafeDisk-V sollte das Programm ViPNet Monitor bereits gestartet sein. Wenn das Programm ViPNet Monitor nicht gestartet oder in der Konfiguration „Internet“ oder „Offenes Internet“ gestartet ist, dann wird eine entsprechende Meldung angezeigt und das Ausführen des Programms ViPNet SafeDisk-V wird nicht möglich sein.

Führen Sie einen der folgenden Schritte aus, um das Programmfenster zu schließen:

- Klicken Sie auf die Schaltfläche im oberen rechten Teil des Fensters.
- Drücken Sie die Tastenkombination **Alt+F4**.

  Beim Versuch, das Programm zu schließen, wird das Fenster **Schließen des Fensters ViPNet SafeDisk** eingeblendet, in welchem Sie eine der zwei Aktionen ausführen können: Hauptfenster ausblenden oder Programm beenden. Wählen Sie die Option **Das Hauptfenster ausblenden, ohne dabei SafeDisk zu beenden** und klicken Sie auf **OK**.



Hinweis. Damit beim Klicken auf die Schaltfläche die gewählte Aktion ohne weitere Rückfragen durchgeführt wird, aktivieren Sie das Kontrollkästchen Dieses Fenster nicht mehr anzeigen. Die vorzunehmende Aktion beim Schließen des Fensters kann in den Programmeinstellungen konfiguriert werden (s. Parameter von ViPNet SafeDisk-V einstellen auf S. 58).

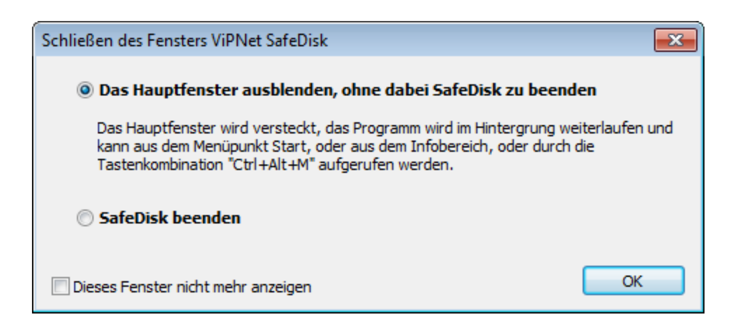


Abbildung 5: Schließen des Fensters ViPNet SafeDisk-V



Tipp. Wenn Sie vorhaben, den Rechner für einige Zeit unbeaufsichtigt laufen zu lassen, empfiehlt es sich, die Option **SafeDisk beenden** auszuwählen.

Außerdem können Sie das Programm so einstellen, dass Container, mit denen aktuell nicht gearbeitet wird, automatisch getrennt werden. Dazu wählen Sie im Menü **SafeDisk** den Befehl **Einstellungen**. Aktivieren Sie im Fenster **Einstellungen** in Registerkarte **Allgemein** das Kontrollkästchen **Container trennen bei Inaktivität länger als**. Details s. Kapitel Parameter von ViPNet SafeDisk-V einstellen.

Führen Sie eine der folgenden Aktionen aus, um das Programmfenster wieder einzublenden:

- Klicken Sie im Infobereich der Taskleiste auf das Symbol .
- Drücken Sie die Tastenkombination **Strg+Alt+M**.
- Doppelklicken Sie auf dem Desktop die Verknüpfung .

Führen Sie einen der folgenden Schritte aus, um das Programm ViPNet SafeDisk-V zu beenden:

- Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Symbol  und wählen Sie den Befehl **Beenden**.
- Wählen Sie im Hauptfenster im Menü **SafeDisk** den Befehl **Beenden**.

Beim Beenden von ViPNet SafeDisk-V trennt das Programm alle eingebundenen Container. Wenn aus irgendwelchen Gründen einige Container nicht getrennt werden können (zum Beispiel, weil die im Container enthaltenen Dateien von anderen Anwendungen benutzt werden), wird vom Programm eine entsprechende Warnung ausgegeben.

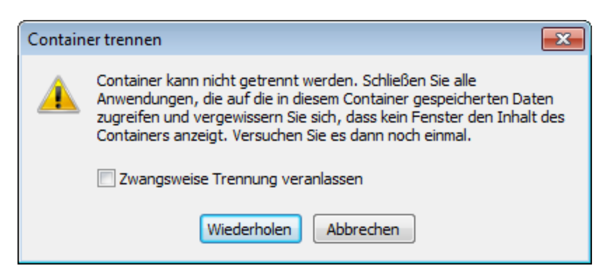


Abbildung 6: Meldung über das Auftreten eines Fehlers beim Trennen eines Containers

Beim Einblenden einer solchen Meldung:

1. Stellen Sie sicher, dass die im Container enthaltenen Dateien nicht von anderen Programmen verwendet werden, und klicken Sie auf **Wiederholen**.
2. Um die Container zwangsweise zu trennen, aktivieren Sie im Meldungsfenster das Kontrollkästchen **Zwangsweise Trennung veranlassen** und klicken Sie auf **Wiederholen**. Das Programm blendet eine Warnung über möglichen Datenverlust ein.



Abbildung 7: Warnung über möglichen Datenverlust

3. Stellen Sie sicher, dass alle im Container enthaltenen Daten abgespeichert sind, und klicken Sie im Meldungsfenster auf **Ja**.



Hinweis. Wenn die im Container enthaltenen Daten nicht abgespeichert werden, kann dies bei einer zwangsweisen Trennung des Containers zum Datenverlust führen.

Beim zwangsweisen Trennen des Containers werden offene Dokumente nicht geschlossen. Diese Dokumente sollten eigenständig geschlossen werden.

Deinstallation von ViPNet SafeDisk-V

Bevor Sie ViPNet SafeDisk-V deinstallieren:

1. Erstellen Sie eine Sicherungskopie Ihrer vertraulichen Daten. Führen Sie dazu einen der folgenden Schritte aus:
   - Kopieren Sie die Container-Dateien und die Sicherungskopien der Containerschlüssel an einen sicheren Ort.
   - Erstellen Sie Export-Dateien für alle Ihre Container und kopieren Sie diese an einen sicheren Ort.
2. Wenn Sie nicht wollen, dass auf dem Computer Spuren sensibler Daten übrigbleiben:
   - Verwenden Sie die Bereinigungsfunktion von ViPNet SafeDisk-V (s. Spurenbeseitigung bei der Arbeit mit privaten Daten auf S. 106).
   - Aktivieren Sie den „Extreme Gefahr“ Modus (s. Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus auf S. 102) und löschen Sie alle Ihre Container und Containerschlüssel.

Zum Deinstallieren von ViPNet SafeDisk-V:

1. Melden Sie sich im Programm ab (s. ViPNet SafeDisk-V beenden auf S. 26).
2. Öffnen Sie über das Menü **Start** die **Systemsteuerung**. Klicken Sie dort auf **Programme und Funktionen** (in Windows XP auf **Software**).
3. Wählen Sie in der Liste der installierten Programme den Eintrag **ViPNet SafeDisk** und klicken Sie auf **Ändern/Entfernen**. Es wird der Assistent **Hinzufügen/Entfernen** gestartet.
4. Aktivieren Sie das Optionsfeld **Alle Komponenten entfernen** und klicken auf **Weiter**.
5. Auf der Seite **Vorbereitung abgeschlossen** klicken Sie auf **Fertig**. Es wird eine Meldung über verbliebene Dateien und Ordner des Benutzers eingeblendet.

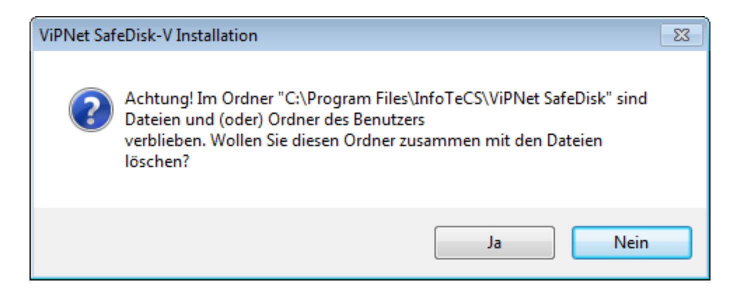


Abbildung 8: Meldung über übriggebliebene Dateien und Ordner des Benutzers

6 Wenn Sie vorhaben, in Zukunft wieder mit den Containern zu arbeiten, klicken Sie auf **Nein**. Wenn Sie auf **Ja** klicken, werden die Daten vollständig gelöscht.

7 Damit der Vorgang der Deinstallation von ViPNet SafeDisk-V abgeschlossen werden kann, muss der Computer neu gestartet werden. Klicken Sie im Fenster mit der Meldung über einen möglichen Neustart des Computers auf die Schaltfläche **Jetzt neu starten**, um den Rechner sofort nach Abschluss der Deinstallation neu zu starten.

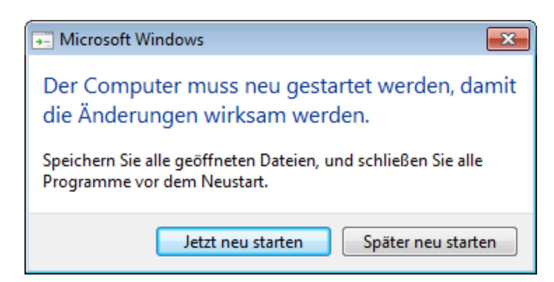


Abbildung 9: Benachrichtigung über den Neustart

Wenn Sie den Computer zu einem späteren Zeitpunkt neu starten wollen, klicken Sie auf **Später neu starten**.



Datenschutz mit Hilfe von ViPNet SafeDisk-V

Vorgehensweise beim Datenschutz

Für den erfolgreichen Schutz von Daten und die Sicherstellung eines sicheren Zugangs zu Informationen müssen alle Schritte aus der nachfolgenden Liste durchgeführt werden.



Hinweis. Einige Punkte dieser Liste beziehen sich auf die Unterpunkte verschiedener Abschnitte. Nach der Durchführung der Unterpunkte wechseln Sie zum nächsten Schritt aus der Liste.

Wenn die Verknüpfung sich auf einen Abschnitt bezieht der allgemeine Information beinhaltet, machen Sie sich mit diesen Informationen vertraut und wechseln Sie zum nächsten Punkt aus der Liste.

	Aufgabe	Verknüpfung
☐	Ein oder mehrere Container erstellen	Container erstellen (auf S. 34)
☐	Sicherungskopien der Containerschlüssel erstellen	Sicherungskopie der Containerschlüssel erstellen (auf S. 39)
☐	Sicherungskopien der Konfiguration regelmäßig erstellen	Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen (auf S. 79)
☐	Regelmäßig Exportdateien des Containers erstellen	Container exportieren (auf S. 65)
☐	Vorbereitung zur Arbeit unter potentiell unsicheren Bedingungen	Vorbereitung für den Einsatz in einer unsicheren Umgebung: Vorgehensweise (auf S. 98)
☐	Stets vollständige Bereinigung durchführen, um alle Spuren der Arbeit mit vertraulichen Daten zu beseitigen	Bereinigung von Datenspuren: Reihenfolge der Schritte (auf S. 111)



Tipp. Es wird empfohlen, die Liste auszudrucken und die einzelnen Punkte nach ihrer Abarbeitung zu markieren.

Container erstellen

Der Assistent **Erstellen des Containers** wird automatisch beim Start von ViPNet SafeDisk-V gestartet, wenn im Programm noch kein Container erstellt wurde.

Zum Erstellen eines neuen Containers:

1 Führen Sie einen der folgenden Schritte durch:

- Klicken Sie auf die Schaltfläche **Erstellen** in der Symbolleiste des Programms.
- Wählen Sie im Menü **Container** den Befehl **Erstellen**.
- Drücken Sie die Taste **Einfg**.

Es wird der Assistent **Erstellen des Containers** gestartet.

2 Klicken Sie im Fenster **Erstellen des Containers** auf die Schaltfläche und geben den Pfad zur Datei des neuen Containers sowie seinen Namen an. Sie können auch die Standardwerte für Pfad und Dateinamen übernehmen.



Abbildung 10: Assistent „Erstellen des Containers“

Zum Fortfahren klicken Sie auf **Weiter**.

3 Auf der Seite **Container-Eigenschaften**:

- Geben Sie im Feld **Container-Größe** die Größe des neuen Containers an.
- Bei der Definition der Container-Größe gelten folgende Einschränkungen:

- Die Größe des Containers muss in einem Bereich zwischen 1024 KB (1 MB) und 2048 GB liegen.
- Wenn die Container-Größe weniger als 3 MB beträgt, kann der Container nicht mit dem NTFS-Dateisystem formatiert werden.
- Wenn die Container-Größe mehr als 2048 MB (2 GB) beträgt, kann der Container nicht mit dem FAT-Dateisystem formatiert werden.
- Wenn die Container-Größe weniger als 68 MB oder mehr als 32 GB beträgt, kann der Container nicht mit dem FAT32-Dateisystem formatiert werden.



Hinweis. Der Dateisystemtyp des Containers sollte bei seiner Formatierung angegeben werden. Wir empfehlen jedoch, die Größe und den Dateisystemtyp bereits beim aktuellen Schritt zu überlegen.

Der Formatierungsvorgang kann in Abhängigkeit von der Containergröße und der Leistungsfähigkeit des Computers einige Minuten bis einige Stunden dauern.

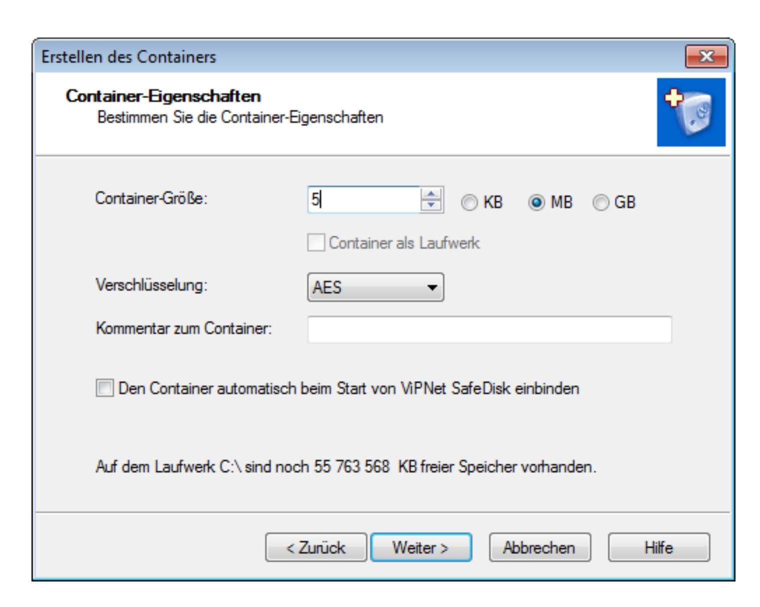


Abbildung 11: Container-Eigenschaften

- Beim Erstellen des Containers auf einem externen Datenträger steht die Funktion zur Verfügung, den Container als ein vollständiges Laufwerk anzulegen. Wenn das Kontrollkästchen **Container als Laufwerk** aktiviert wird, dann ist die Angabe der Speichergröße für den zu erstellenden Container nicht mehr nötig. Die Größe des neuen Containers wird in diesem Fall dem Speichervolumen des externen Datenträgers entsprechen. Bei Verwendung dieser Funktion werden alle Daten, die auf dem externen Gerät gespeichert sind, unwiderbringlich gelöscht. Deswegen empfehlen wir

Ihnen, rechtzeitig Sicherungskopien aller benötigten Daten zu erstellen und den Gerätespeicher vor dem Erstellen eines Containerlaufwerks zu leeren.



Hinweis. Wenn das Dateisystem auf dem Datenträger eine Dateigröße, die dem Volumen des Datenträgers entspricht, nicht unterstützt, dann sollte der Datenträger vorab in einem anderen Dateisystem formatiert werden. Ein externer Datenträger mit einem Speichervolumen von 16 GB, der im Dateisystem FAT32 formatiert ist, sollte zum Beispiel zuvor im Dateisystem NTFS formatiert werden, da das Dateisystem FAT32 eine Dateigröße von mehr als 4 GB nicht unterstützt.

- Aus der Dropdown-Liste **Verschlüsselung** wählen Sie den Verschlüsselungsalgorithmus für diesen Container. Sie können zwischen AES und GOST wählen.



Hinweis. AES und GOST sind symmetrische Verschlüsselungsalgorythmen. AES ist der staatliche Verschlüsselungsstandard in den USA. GOST ist der staatliche Verschlüsselungsstandard in der Russischen Föderation und ist als GOST 28147-89 standardisiert.

- Im Feld **Kommentar zum Container** können Sie einen beliebigen Kommentar eingeben. Dieser wird im Programmfenster von ViPNet SafeDisk-V rechts vom Containernamen abgebildet. Kurze, durchdachte Beschreibungen können dabei helfen, den benötigten Container schneller zu finden.
- Wenn Sie wollen, dass der Container automatisch beim Start von ViPNet SafeDisk-V eingebunden wird, aktivieren Sie das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden**.



Tipp. Wenn Sie das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden** nicht aktiviert haben, können Sie diese Einstellung später in den Container-Eigenschaften ändern.

1 Klicken Sie auf **Weiter**. Es wird nun das digitale Roulette geöffnet (wenn es nicht bereits früher in der aktuellen Sitzung von ViPNet SafeDisk-V gestartet wurde).

Das digitale Roulette initialisiert den Zufallszahlengenerator. Zufallszahlen werden zum Erzeugen von Containerschlüsseln gebraucht. Das digitale Roulette wird nur einmal während der Arbeitssitzung von ViPNet SafeDisk-V gestartet, wenn zum ersten Mal die Notwendigkeit besteht, eine zufällige Zahl zu erzeugen.

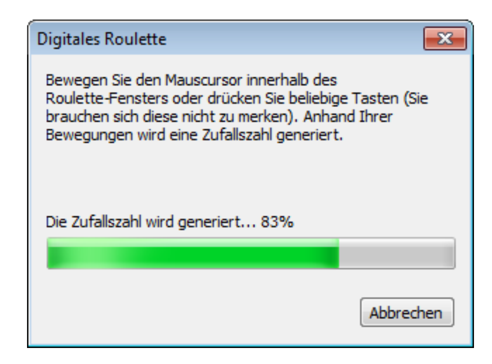


Abbildung 12: Digitales Roulette

Folgen Sie den Anweisungen im Fenster **Digitales Roulette**. Auf diese Weise werden die Schlüssel des Containers erstellt.

2 Klicken Sie auf der Seite **Abschluss der Erstellung des Containers** auf die Schaltfläche **Fertig**. Wenn das Kontrollkästchen **Erstellung einer Sicherungskopie der Containerschlüssel starten** aktiviert ist, wird anschließend automatisch der Assistent **Erstellen der Sicherungskopie der Containerschlüssel** gestartet (s. Sicherungskopie der Containerschlüssel erstellen auf S. 39).

Wenn dieses Kontrollkästchen deaktiviert wurde, bindet das Programm den neu erstellten Container automatisch ein und schlägt seine Formatierung vor.



Abbildung 13: Abschluss der Erstellung des Containers

Dadurch wird im von Ihnen angegebenen Ordner die versteckte Container-Datei `*.sdc` (s. Container-Datei auf S. 143) erzeugt. Zum Anzeigen dieser Datei öffnen Sie in der Systemsteuerung das Fenster **Ordner- und Suchoptionen** und aktivieren Sie auf der

Registerkarte **Ansicht** die entsprechende Option unter dem Eintrag **Versteckte Dateien und Ordner**.



Achtung! In der aktuellen Version des Programms kann die Datei mit Komprimierungs- und Verschlüsselungsattributen nicht als SafeDisk-V-Container benutzt werden.

Sicherungskopie der Containerschlüssel

Eine Sicherungskopie der Containerschlüssel kann in folgenden Fällen erforderlich sein:

- Sie erhalten keinen Zugang zum Container, obwohl die Container-Datei nicht beschädigt ist;
- Sie wollen den Containerzugang für einen anderen Benutzer, der auf Ihrem Computer registriert ist, ermöglichen;
- Sie wollen die Container-Datei *.sdc manuell kopieren (ohne Verwendung der Export-Funktionalität des Containers).



Achtung! Sie können die Sicherungskopie der Containerschlüssel für die Wiederherstellung des Zugangs zu geschützten Daten verwenden, wenn die Containerschlüssel beschädigt wurden. Wenn die Container-Datei selbst beschädigt wurde, können die darin enthaltenen Daten nur durch einen Import der Container-Datei wiederhergestellt werden (wenn zu einem früheren Zeitpunkt eine Exportdatei dieses Containers erstellt wurde).

Deswegen wird ausdrücklich empfohlen, regelmäßig vollständige Sicherungskopien aller Container zu erstellen (s. Container exportieren auf S. 65).

Sicherungskopie der Containerschlüssel erstellen

1. Klicken Sie auf der ersten Seite des Assistenten **Erstellen der Sicherungskopie der Containerschlüssel** (s. Sicherungskopie der Containerschlüssel auf S. 145) auf **Weiter**.
2. Auf der Seite **Art der Speicherung der Sicherungskopie der Containerschlüssel** gehen Sie wie folgt vor:

- Wenn Sie die Sicherungskopie in einer Datei auf dem Computer speichern wollen, wählen Sie in der Liste **Art der Speicherung** den Eintrag **Datei** aus.

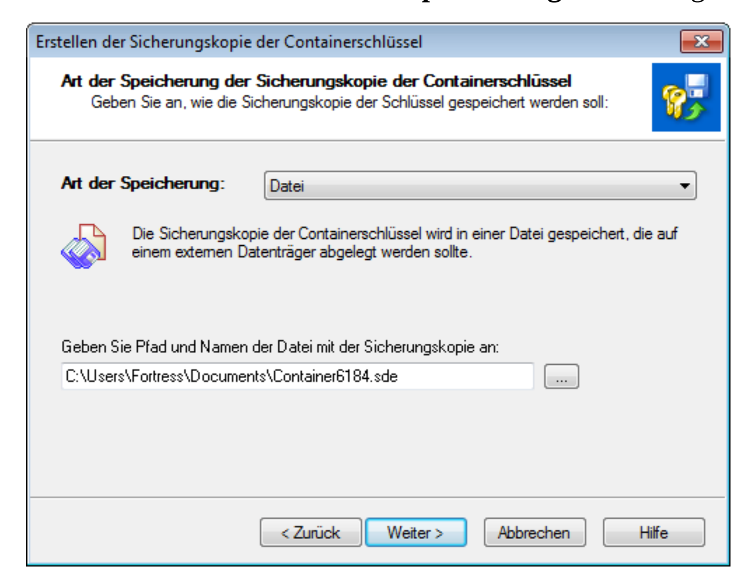


Abbildung 14: Sicherungskopie der Schlüssel in einer Datei speichern

Klicken Sie auf  und geben Sie den Ordner an, in welchem Sie die Sicherungskopie der Schlüssel speichern wollen. Sie können auch den standardmäßig vorgeschlagenen Ordner übernehmen. Klicken Sie anschließend auf **Weiter**.

Tipp. Speichern Sie die Sicherungskopie der Containerschlüssel aus Sicherheitsgründen nicht in demselben Ordner ab, in dem sich die Container-Datei befindet. Wir empfehlen Ihnen, abnehmbares Gerät zum Speichern der Sicherungskopie der Containerschlüssel zu nutzen.

- Wenn Sie die Sicherungskopie auf einem Authentisierungsgerät speichern wollen:
  - Wählen Sie in der Liste **Art der Speicherung** den Eintrag **Authentisierungsgerät** aus.
  - Geben Sie im Feld **Name der Sicherungskopie der Schlüssel** den Namen der Sicherungskopie ein.
  - Stellen Sie sicher, dass das Authentisierungsgerät mit der entsprechenden Leseeinrichtung verbunden ist.
  - Wählen Sie in der Liste **Gerät** das verwendete Authentisierungsgerät aus (wenn es nicht bereits automatisch ausgewählt wurde).

- Geben Sie im Feld **Geben Sie die PIN ein** die PIN für das Authentisierungsgerät ein. Um die PIN zu speichern, aktivieren Sie das entsprechende Kontrollkästchen.
- Klicken Sie auf **Weiter**.



Abbildung 15: Sicherungskopie auf einem Authentisierungsgerät speichern

3 Geben Sie auf der Seite **Zugangspasswort** das Kennwort für die Sicherungskopie ein und wiederholen zur Bestätigung die Eingabe. Klicken Sie auf **Weiter**.

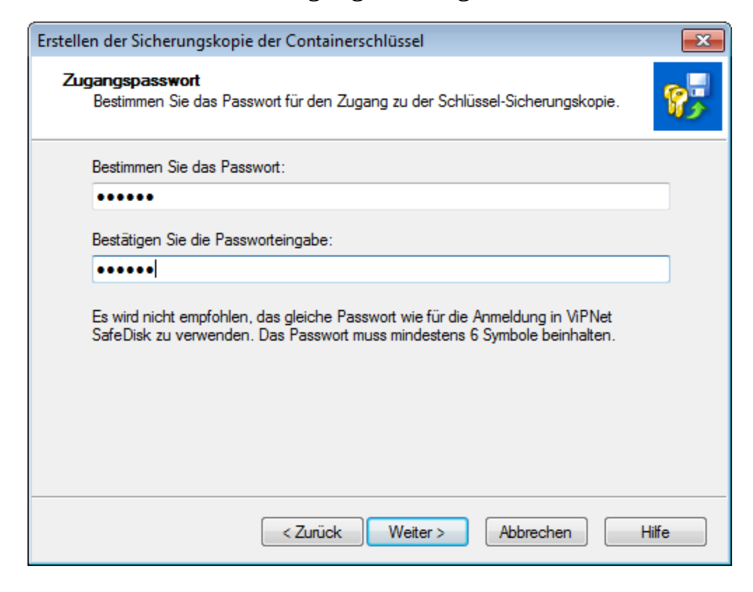


Abbildung 16: Kennwort für den Zugang zur Sicherungskopie der Containerschlüssel einrichten

4 Klicken Sie auf der Seite **Abschluss der Erstellung der Sicherungskopie der Containerschlüssel** auf **Fertig**.

Es wird entweder eine Datei mit der Erweiterung `*.sde` erstellt, die die Sicherungskopie der Containerschlüssel enthält oder die Sicherungskopie der Containerschlüssel wird auf dem Authentisierungsgerät abgelegt.

Assistenten zur Erstellung von Sicherungskopien der Containerschlüssel starten

Wenn Sie eine Sicherungskopie der Schlüssel für einen Container erstellen möchten, der bereits existiert, führen Sie zum Starten des Assistenten **Erstellen der Sicherungskopie der Containerschlüssel** die folgenden Schritte aus:

1. Wählen Sie im Programmfenster von ViPNet SafeDisk-V den Container aus, für welchen eine Sicherungskopie der Schlüssel erstellt werden soll.
2. Wenn der Container eingebunden ist, trennen Sie ihn.
3. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie im Menü **Container** den Eintrag **Sicherungskopie der Containerschlüssel**.
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Sicherungskopie der Schlüssel**.

   Es wird der Assistent **Erstellen der Sicherungskopie der Containerschlüssel** gestartet.

Container einbinden

Damit der Zugriff auf geschützte Daten, die im Container enthalten sind, möglich wird, muss der Container zunächst eingebunden werden. Ein Container kann nur dann eingebunden werden, wenn die Verwendung von SafeDisk-V-Containern in der aktuellen Konfiguration von ViPNet Monitor erlaubt ist.

Wenn die Einbindung von Containern erlaubt ist, schlägt das Programm beim Erstellen eines neuen Containers vor, diesen automatisch einzubinden (s. Container erstmalig einbinden auf S. 44).

Zum Einbinden eines früher angelegten Containers gehen Sie wie folgt vor:

1. Wählen Sie im Programmfenster von ViPNet SafeDisk-V den Container aus, der eingebunden werden soll.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Einbinden** .
   - Wählen Sie im Menü **Container** den Befehl **Einbinden**.
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Befehl **Einbinden**.
   - Drücken Sie die Taste **C**.
3. Führen Sie im Fenster **Einbinden Container...** die folgenden Schritte aus:
   - Wählen Sie in der Liste **Container einbinden als Laufwerk** einen Buchstaben für das Laufwerk aus, das den Container unter Windows repräsentieren soll.



Abbildung 17: Container einbinden

- Wenn Sie den Container sofort in einem separaten Fenster öffnen wollen, aktivieren Sie das Kontrollkästchen **Das Fenster mit dem Containerinhalt öffnen**.
- Wenn Sie verhindern möchten, dass der Inhalt des Containers während der Arbeitssitzung modifiziert werden kann, aktivieren Sie das Kontrollkästchen **Container nur zum Lesen einbinden**.
- Wenn Sie unter Windows XP oder Windows Server 2003 arbeiten und möchten, dass niemand außer Ihnen Zugang zum Container besitzt, dann aktivieren Sie das Kontrollkästchen **Exklusiver Zugriff**.

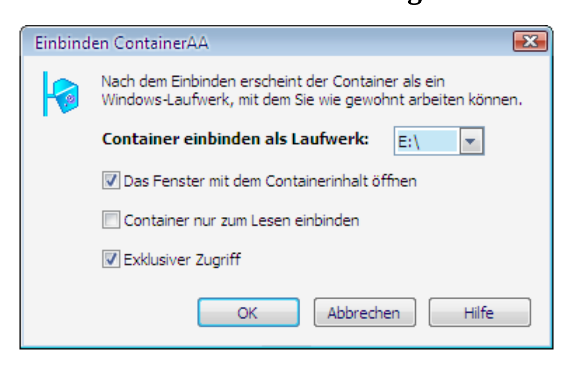


Abbildung 18: Exklusiver Zugriff aktivieren



Hinweis. Beim Verwenden der Option **Exklusiver Zugriff** kann der Container nicht ausschließlich zum Lesen eingebunden werden.

4 Klicken Sie auf **OK**.

Der Container wird als neues lokales Laufwerk eingebunden.

Container erstmalig einbinden

Wenn in der aktuellen Konfiguration von ViPNet Monitor die Verwendung der SafeDisk-V-Container erlaubt ist, schlägt das Programm nach der Erstellung eines neuen Containers mitsamt einer Sicherungskopie seiner Schlüssel vor, den neu angelegten Container sofort einzubinden.

Zum Einbinden des Containers:

1 Klicken Sie im Fenster mit dem Vorschlag, den Container einzubinden, auf **Ja**.

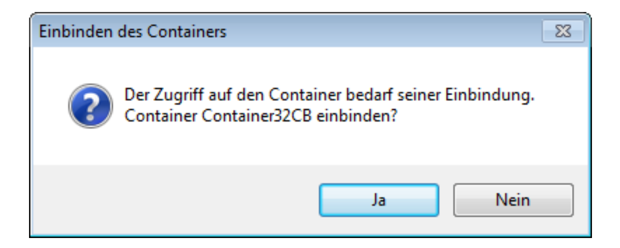


Abbildung 19: Vorschlag zur Einbindung des Containers

2 Geben Sie im Fenster **Einbinden** (s. Abbildung auf S. 43) die Parameter für die Einbindung an.



Hinweis. Aktivieren Sie beim Erstellen eines neuen Containers nicht das Kontrollkästchen **Container nur zum Lesen einbinden**, da es dadurch nicht möglich sein wird, den Container anschließend zu formatieren. Wenn Sie dieses Kontrollkästchen trotzdem aktiviert haben, trennen Sie entweder den Container und binden Sie ihn erneut ein oder legen Sie den Container neu an, ohne dabei das Kontrollkästchen zu aktivieren.

3 Klicken Sie auf **OK**. Bei der erstmaligen Einbindung des Containers wird der Assistant zur Container-Formatierung gestartet (s. Container formatieren auf S. 46).

Container formatieren

Vor Beginn der Nutzung muss ein Container formatiert werden. Bei Einbindung eines nicht formatierten Containers wird automatisch der Assistent **Container formatieren** gestartet. Zum Formatieren eines Containers:

1 Wählen Sie auf der ersten Seite des Assistenten in der Liste Dateisystem das richtige Dateisystem für die Formatierung aus.



Hinweis. Die Wahl des Dateisystems hängt von der Containergröße ab:

- Das Dateisystem FAT kann ausgewählt werden, falls die Containergröße mehr als 1 MB und weniger als 2 GB beträgt.
- Das Dateisystem FAT32 kann ausgewählt werden, falls die Containergröße mehr als 32 MB und weniger als 4 GB beträgt.
- Das Dateisystem NTFS kann ausgewählt werden, falls die Containergröße mehr als 3 MB beträgt.



Achtung! In Windows 8 kann ein Container ausschließlich mit Hilfe der Betriebssystemmittel in FAT32 formatiert werden.



Abbildung 20: Assistent für die Container-Formatierung

2 Klicken Sie auf **Weiter**, um mit der Formatierung zu beginnen.



Hinweis. Der Vorgang der Formatierung kann einige Minuten oder einge Stunden dauern, abhängig von der Containergröße und der Computerleistung. Wenn die zum Formatieren eines Containers erforderliche Zeit eingeschätzt werden soll, empfehlen wir, zunächst einen kleinen Container (z. B. 1 GB) zu erstellen und die Zeit bei seiner Formatierung zu messen.

3 Nach Abschluss der Formatierung klicken Sie auf der letzten Seite des Assistenten auf die Schaltfläche **Fertig**. Der Container ist nun einsatzbereit.

Geschützte Daten alltäglich verwenden

Nachdem Sie alle Container angelegt haben, können Sie sich bei der alltäglichen Arbeit mit geschützten Daten an die folgende Vorgehensweise halten:

1. Stellen Sie sicher, dass im Programm ViPNet Monitor eine Konfiguration eingestellt ist, bei der die Verwendung von SafeDisk-V-Containern erlaubt ist.
2. Starten Sie ViPNet SafeDisk-V, indem Sie auf dem Desktop auf das Programmsymbol doppelklicken oder den Eintrag **ViPNet SafeDisk** über das Menü **Start** auswählen. Es wird das Anmeldefenster des Programms geöffnet.
3. Führen Sie die Anmeldung im Programm gemäß den Anweisungen in Kapitel Benutzerauthentisierungsmodi in ViPNet SafeDisk durch.

   Es wird das Hauptprogrammfenster von ViPNet SafeDisk-V geöffnet.
4. Wählen Sie im Programmfenster von ViPNet SafeDisk-V den Container aus, der die benötigten Daten enthält.
5. Klicken Sie auf **Einbinden** , um den Container einzubinden. Es wird das Fenster **Einbinden** (s. Abbildung auf S. 43) eingeblendet. Geben Sie die Parameter für die Einbindung an und klicken auf **OK**.

   Mehr über das Einbinden des Containers s. Kapitel Container einbinden (auf S. 43).

   Doppelklicken Sie auf den eingebundenen Container. In einem separaten Fenster wird das Container-Laufwerk angezeigt. Sie können nun mit dem Container wie mit einem gewöhnlichen Windows-Laufwerk arbeiten: Daten, die Sie schützen möchten, dort abspeichern oder Dokumente auf dem Laufwerk ablegen und editieren.



Hinweis. Wenn das Programm ViPNet SafeDisk-V unter dem Betriebssystem Windows XP installiert ist und der Container in das NTFS-Dateisystem formatiert wurde, dann verfügt nur der Betriebssystemadministrator von Windows XP über das Recht, Dateien im Stammordner des Containerlaufwerks zu erstellen. Benutzer, die keine Administratorrechte unter Windows XP besitzen, können die benötigten Ordner im Stammverzeichnis des Containerlaufwerks im Voraus erstellen und anschließend mit den Dateien innerhalb dieser Ordner arbeiten.



Achtung! Es wird empfohlen, während der Arbeit mit Containern die automatische Installation von Updates, die vom ViPNet Updatesystem an die Programme ViPNet Client oder ViPNet Coordinator weitergeleitet werden, zu deaktivieren. Das Update kann erst installiert werden, nachdem die Arbeit mit Containern abgeschlossen ist.

6 Wenn Sie die Arbeit mit geschützten Daten beenden wollen, schließen Sie zunächst alle Dateien, die im Container enthalten sind, sowie alle Fenster, die den Containerinhalt abbilden. Wählen Sie anschließend im Programmfenster den benötigten Container aus und klicken Sie auf die Schaltfläche **Trennen** . Nach dem Trennen des Containers ist der Zugang zu geschützten Daten nicht mehr möglich, und die Präsenz dieser Daten auf dem Rechner ist nicht mehr offensichtlich.

7 Melden Sie sich in ViPNet SafeDisk-V ab (s. ViPNet SafeDisk-V beenden auf S. 26).

Containersymbole in ViPNet SafeDisk-V

In der nachfolgenden Tabelle sind die Containersymbole von ViPNet SafeDisk-V samt ihrer Beschreibung aufgelistet.

Tabelle 3. Beschreibung der Containersymbole von SafeDisk-V

Containersymbol in SafeDisk-V	Symbolbeschreibung
	Container ist bereit, aber nicht eingebunden.
	Container ist bereit und eingebunden. Er kann wie ein gewöhnliches Windows-Laufwerk verwendet werden.
	Container ist erstellt, aber gegenwärtig nicht verfügbar (möglicherweise wurde die Container-Datei auf einem abnehmbaren Datenträger angelegt, zu dem nun kein Zugang besteht).
	Container ist beschädigt, da entweder die Container-Datei selbst oder die Containerschlüssel beschädigt sind. Ausführliche Informationen dazu finden Sie in Kapitel Wiederherstellen des Zugriffs auf die geschützten Daten (auf S. 75).

Container trennen

Damit Ihre privaten Daten verborgen bleiben, sollten die Container getrennt werden. Außerdem können einige Aktionen nur mit getrennten Containern durchgeführt werden, zum Beispiel die Änderung der Container-Eigenschaften, der Export des Containers oder die Erstellung einer Sicherungskopie der Containerschlüssel.

Zum Trennen des Containers:

1. Wählen Sie im Hauptfenster den Container aus, der getrennt werden soll. Eingebundene Container werden durch das Symbol gekennzeichnet, getrennte durch das Symbol .

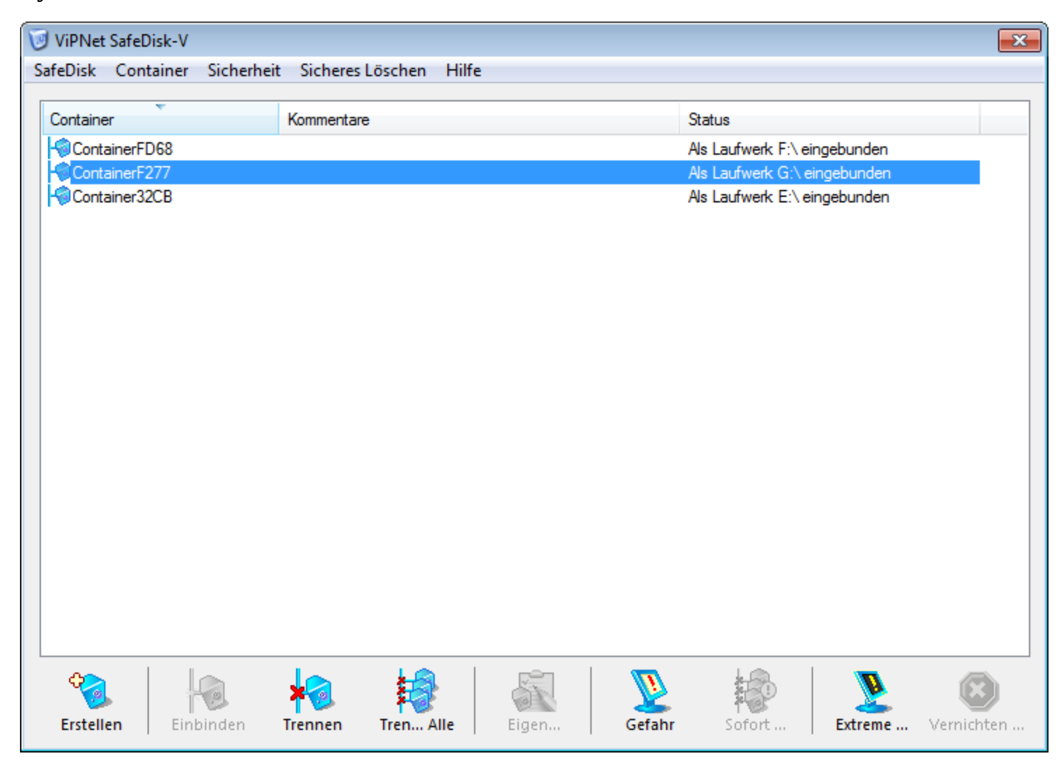


Abbildung 21: Eingebundene und getrennte Container

2. Schließen Sie alle Dateien, die im Container gespeichert sind, sowie alle Fenster, die den Containerinhalt abbilden.

3. Führen Sie im Programmfenster von ViPNet SafeDisk-V einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Trennen**  .
- Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Befehl **Trennen**.

- Wählen Sie im Menü Container den Befehl **Trennen**.
- Drücken Sie die Taste **D**.

Wenn Sie alle Container gleichzeitig trennen wollen, führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Alle trennen** .
- Wählen Sie im Menü Container den Befehl **Alle trennen**.
- Drücken Sie die Tastenkombination **Alt+D**.

4 Wenn der Container aus irgendwelchen Gründen nicht getrennt werden kann (zum Beispiel wenn die im Container enthaltenen Dateien von anderen Anwendungen benutzt werden), wird vom Programm eine entsprechende Warnung ausgegeben.

Damit der Container zwangsweise getrennt wird, aktivieren Sie im Meldungsfenster das Kontrollkästchen **Zwangsweise Trennung veranlassen** und klicken Sie auf **Wiederholen**.



Achtung! Bei einer zwangsweisen Trennung des Containers werden geöffnete Dokumente nicht geschlossen. Diese Dokumente sollten Sie eigenhändig schließen.

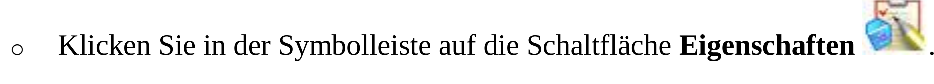


Tipp. Damit beim Näherkommen Unbefugter alle Container sofort getrennt werden können, aktivieren Sie den „Gefahr“-Modus (s. Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus auf S. 99).

Container-Eigenschaften anzeigen und ändern

Führen Sie die folgenden Schritte aus, um Container-Eigenschaften anzuzeigen und (oder) zu ändern:

1. Wählen Sie im Hauptfenster von ViPNet SafeDisk-V den passenden Container aus und trennen ihn.
2. Führen Sie einen der nachfolgenden Schritte aus:



   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften** .
   - Wählen Sie im Menü **Container** den Befehl **Eigenschaften**.
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Eigenschaften**.
   - Drücken Sie die Tastenkombination **Alt+Eingabe**.

3. Im Fenster **Eigenschaften** können Sie in der Registerkarte **Container** die wichtigsten Parameter des gewählten Containers ändern:
   - Namen und Pfad des Containers (s. Container-Datei verschieben auf S. 56);
   - Kommentar zum Container;
   - Das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden** aktivieren oder deaktivieren;

     Beim Aktivieren dieser Option wird der Container beim Wechsel zu einer ViPNet Monitor Konfiguration, in der die automatische Einbindung von Containern erlaubt ist, sowie beim Start von ViPNet SafeDisk-V in einer entsprechenden Konfiguration automatisch eingebunden. Weitere Details über Änderungen der Konfigurationseinstellungen finden Sie im Dokument „ViPNet Client Monitor. Benutzerhandbuch“.
   - Das Kontrollkästchen **Nur zum Lesen einbinden** aktivieren oder deaktivieren.

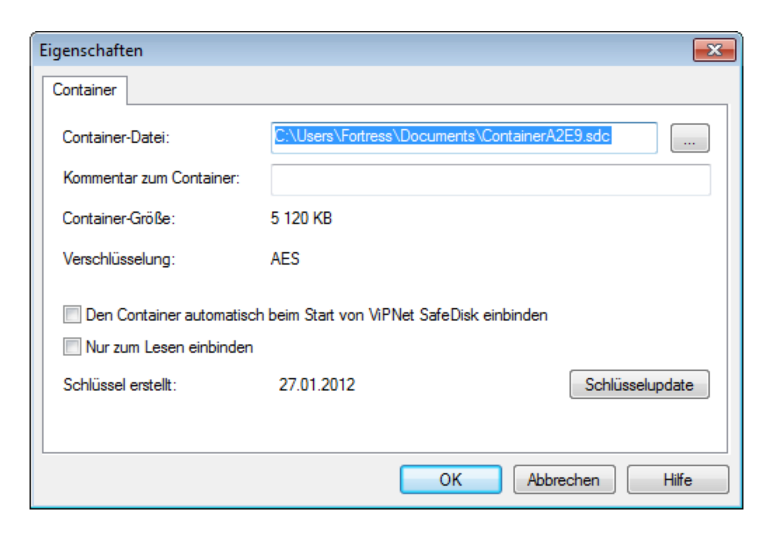


Abbildung 22: Fenster der Container-Eigenschaften



Hinweis. Die Container-Größe sowie der Verschlüsselungsalgorithmus können nicht geändert werden.

---

4 Wenn die Containerschlüssel aktualisiert werden sollen (s. Containerschlüssel aktualisieren auf S. 54), klicken Sie auf die Schaltfläche **Schlüsselupdate**.

5 Nach Durchführung aller erforderlichen Änderungen klicken Sie auf **OK**, um die Einstellungen zu speichern. Wenn Sie die Änderungen nicht übernehmen wollen, klicken Sie auf **Abbrechen**.

Containerschlüssel aktualisieren

Damit die Sicherheit beim Schutz von Daten, die in SafeDisk-V-Containern gespeichert sind, erhöht werden kann, besteht die Möglichkeit zum Aktualisieren der Containerschlüssel (d. h. Schlüssel, mit denen die im Container enthaltenen Daten verschlüsselt werden). Nach dem Update wird der Zugang zum Container mit Hilfe alter Schlüssel (oder einer Sicherungskopie der alten Schlüssel) nicht mehr möglich sein. Es wird empfohlen, das Update der Containerschlüssel nicht seltener als alle 15 Monate durchzuführen. Das Erstellungsdatum der Containerschlüssel wird im Fenster **Eigenschaften** in der Registerkarte **Container** angezeigt.

Zum Aktualisieren des Containerschlüssels:

1. Wählen Sie im Programmfenster von ViPNet SafeDisk-V den Container aus, für welchen die Schlüssel aktualisiert werden sollen.

2. Führen Sie einen der folgenden Schritte durch:

   - Wählen Sie im Menü **Container** den Befehl **Schlüssel aktualisieren**.
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Schlüsselupdate**.

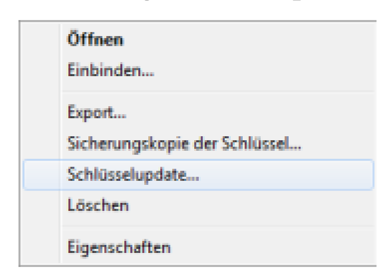
     

     Abbildung 23: Containerschlüsselupdate

   - Klicken Sie im Fenster **Eigenschaften** in der Registerkarte **Container** auf die Schaltfläche **Schlüsselupdate**.

   Es wird der Assistent **Containerschlüssel aktualisieren** gestartet.

3. Klicken Sie auf der ersten Seite des Assistenten **Containerschlüssel aktualisieren** auf die Schaltfläche **Weiter**.

   Es wird eine Seite mit der Fortschrittsanzeige des Update-Vorgangs eingeblendet. Sie können auf **Stopp** klicken, um den Vorgang zu anzuhalten.

4. Nach Abschluss der Schlüsselaktualisierung wird die Seite **Aktualisierung der Containerschlüssel wird abgeschlossen** eingeblendet.

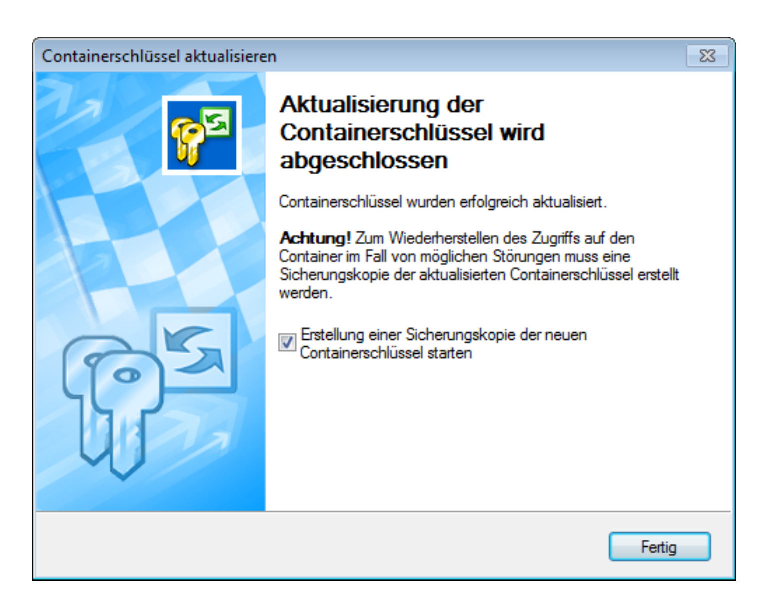


Abbildung 24: Containerschlüssel-Aktualisierung abschließen

Auf dieser Seite ist das Kontrollkästchen **Erstellung einer Sicherungskopie der neuen Containerschlüssel starten** standardmäßig aktiviert. Die Sicherungskopie der neuen Schlüssel wird sofort nach Abschluss des Assistenten angelegt. Deaktivieren Sie dieses Kontrollkästchen, um die Sicherungskopie der neuen Containerschlüssel zu einem späteren Zeitpunkt zu erstellen.



Achtung! Die Sicherungskopie der Containerschlüssel wird für die Wiederherstellung des Containerzugangs im Falle einer Schlüsselbeschädigung verwendet. Deswegen wird es ausdrücklich empfohlen, Sicherungskopien der Containerschlüssel zu erstellen.

Wenn Sie mit Hilfe einer Sicherungskopie der Containerschlüssel anderen Benutzern den Zugang zum Container auf Ihrem Computer gewährt haben (s. Containerzugang für einen oder mehrere Benutzer auf demselben oder auf unterschiedlichen Computern bereitstellen auf S. 88), können diese nach Abschluss der Schlüsselaktualisierung nicht mehr mit dem Container arbeiten. Wenn Sie den Containerzugang wieder bereitstellen wollen, überreichen Sie eine Sicherungskopie der neuen Containerschlüssel an die entsprechenden Benutzer.

---

5 Klicken Sie auf **Fertig**, um die Arbeit des Assistenten abzuschließen.

Container-Datei verschieben

Damit Sie mit den Containern von SafeDisk-V bequem arbeiten können, können die Containerdateien in einen anderen Ordner, auf einen externen Datenträger oder auf ein Remote-Laufwerk kopiert oder auf eine CD geschrieben werden.

Um eine Container-Datei in einen anderen Ordner, auf ein externes Gerät oder ein Netzlaufwerk zu verschieben:

1. Öffnen Sie das Fenster mit den Container-Eigenschaften (s. Container-Eigenschaften anzeigen und ändern auf S. 52).
2. Geben Sie im Fenster **Container-Eigenschaften** in der Registerkarte **Container** im Feld **Container-Datei** den neuen Pfad zur Container-Datei an.
3. Klicken Sie auf **OK**.

Die Datei wird entsprechend dem neuen Pfad verschoben.

Wenn Sie vorhaben, mit Containern zu arbeiten, die auf einer CD gespeichert sind, dann sollte der neue Pfad der Containerdatei nach Abschluss des Schreibvorgangs im Fenster der Containereigenschaften angegeben werden. Auf einen Container, der auf einer CD gespeichert ist, kann nur lesend zugegriffen werden. Deswegen sollte für die ordnungsgemäße Verwendung des Containers das Kontrollkästchen **Nur zum Lesen einbinden** aktiviert werden.



Achtung! ViPNet SafeDisk-V unterstützt die Arbeit mit Container-Dateien, die auf CD im ISO und ISO+Joilet-Format gespeichert werden.

Container löschen

Vergewissern Sie sich vor dem Löschen eines Containers, dass Sie die im Container enthaltenen Daten notfalls wiederherstellen können. Eine Wiederherstellung der Daten ist möglich, falls zumindest eine der nachfolgenden Bedingungen erfüllt ist:

- Eine Exportdatei des Containers wurde erstellt (`*.sdx`).
- Eine Sicherungskopie der Containerschlüssel wurde erstellt (`*.sde`), welche zusammen mit einer Kopie der Container-Datei (`*.sdc`) an einem sicheren Ort aufbewahrt wird.



Achtung! Wenn Sie die oben genannten Dateien nicht angelegt haben, können Sie die Daten aus dem gelöschten Container nicht wiederherstellen.

Zum Löschen des Containers:

1 Trennen Sie den Container, falls er eingebunden ist .

2 Markieren Sie den Container und führen einen der folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Löschen**.
- Wählen Sie im Menü **Container** den Befehl **Löschen**.
- Drücken Sie die Taste **Entf**.

3 Aktivieren Sie im Fenster **Container löschen** die Kontrollkästchen **Ich will diesen Container tatsächlich löschen** und **Es ist mir bewusst, dass die Informationen unwiderruflich gelöscht werden**.



Abbildung 25: Warnung über das Löschen des Containers

4 Klicken Sie auf **Container löschen**.

Parameter von ViPNet SafeDisk-V einstellen

Zum Konfigurieren der Parameter von ViPNet SafeDisk-V:

1 Wählen Sie im Menü **SafeDisk** den Eintrag **Einstellungen**.

2 Öffnen Sie im Fenster **Einstellungen** die Registerkarte **Allgemein**.

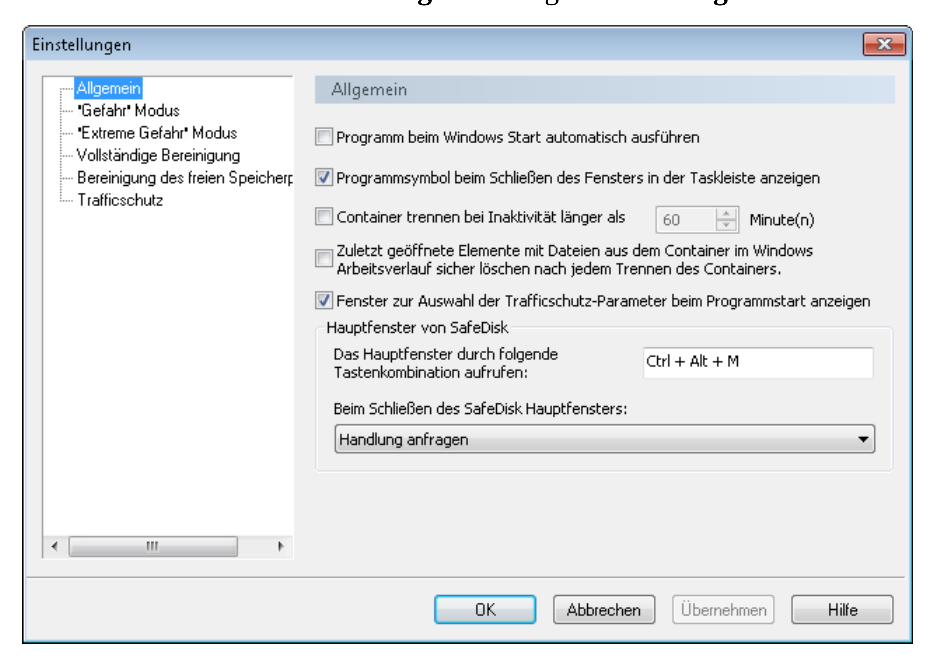


Abbildung 26: Einstellungen von ViPNet SafeDisk-V

3 Wenn Sie möchten, dass ViPNet SafeDisk-V automatisch beim Hochfahren von Windows gestartet wird, dann aktivieren Sie das Kontrollkästchen **Programm beim Windows Start automatisch ausführen**.

4 Wenn Sie nicht wollen, dass das Symbol von ViPNet SafeDisk-V im Infobereich der Taskleiste eingeblendet wird, dann deaktivieren Sie das Kontrollkästchen **Programmsymbol beim Schließen des Fensters in der Taskleiste anzeigen**.

5 Zum Einstellen der Leerlaufzeit, nach deren Ablauf die Container automatisch getrennt werden sollen, aktivieren Sie das Kontrollkästchen **Container trennen bei Inaktivität länger als** und geben die Zeit in Minuten an (standardmäßig ist der Wert 60 eingestellt).

6 Zum Bereinigen des Arbeitsverlaufs von zuletzt geöffneten Dokumenten nach Abschluss der Arbeit aktivieren Sie das Kontrollkästchen **Zuletzt geöffnete Elemente mit Dateien aus dem Container im Windows Arbeitsverlauf sicher löschen**.

7 Um den Hotkey-Tastaturbefehl zum Aufrufen des ViPNet SafeDisk-V Programmfensters zu ändern, klicken Sie in das Eingabefeld **Das SafeDisk Hauptfenster durch folgende Tastenkombination aufrufen** und drücken Sie eine neue Tastenkombination.

8 Wenn Sie möchten, dass das Fenster zur Auswahl der Trafficschutzparameter (s. Abbildung auf S. 25) bei jedem Start des Programms ViPNet SafeDisk-V angezeigt wird, dann aktivieren Sie das Kontrollkästchen **Fenster zur Auswahl der Trafficschutzparameter beim Start einblenden**.

9 Zum Ändern der Aktion, die beim Anklicken der Schaltfläche **Schließen** ausgeführt wird, wählen Sie in der Liste **Beim Schließen des SafeDisk Hauptfensters** eine der folgenden Optionen aus: **Handlung anfragen**, **Das SafeDisk-Fenster verstecken ohne dabei das Programm zu schließen** oder **SafeDisk schließen**.

10 Wenn Sie die vorgenommenen Änderungen beibehalten wollen, klicken Sie auf **Übernehmen** und anschließend auf **OK**. Wenn Sie die Änderungen nicht speichern wollen, klicken Sie auf **Abbrechen**.

Konfiguration der Parameter für die Trafficblockierung bei Verwendung geschützter Container

Damit Sie sicher mit verschlüsselten Containern arbeiten können, haben Sie die Möglichkeit, alle Verbindungen Ihres Knotens mit externen Knoten zu blockieren. Dazu sollten im Programm ViPNet SafeDisk-V die Parameter für die Blockierung des Traffics eingestellt werden. Diese Parameter werden im Programm ViPNet Monitor angewendet. In Abhängigkeit von den gewählten Einstellungen können alle Verbindungen zu geschützten und/oder offenen Knoten vollständig oder teilweise blockiert werden. Die im Programm ViPNet SafeDisk-V definierten Parameter können im Programm ViPNet Monitor nicht geändert werden. Dadurch wird ein zusätzlicher Schutz vor unerlaubten Zugriffen auf geschützte Container sowohl für die Benutzer des offenen als auch für die Benutzer des privaten Netzwerks sichergestellt (z. B. erhält der Netzwerkadministrator oder der ViPNet-Netzwerkadministrator keinen Zugang mehr zum Container).

Zum Konfigurieren der Trafficschutzparameter:

1. Wählen Sie im Menü **SafeDisk** den Eintrag **Einstellungen**.
2. Wechseln Sie im Fenster **Einstellungen** zum Bereich **Trafficschutz**.

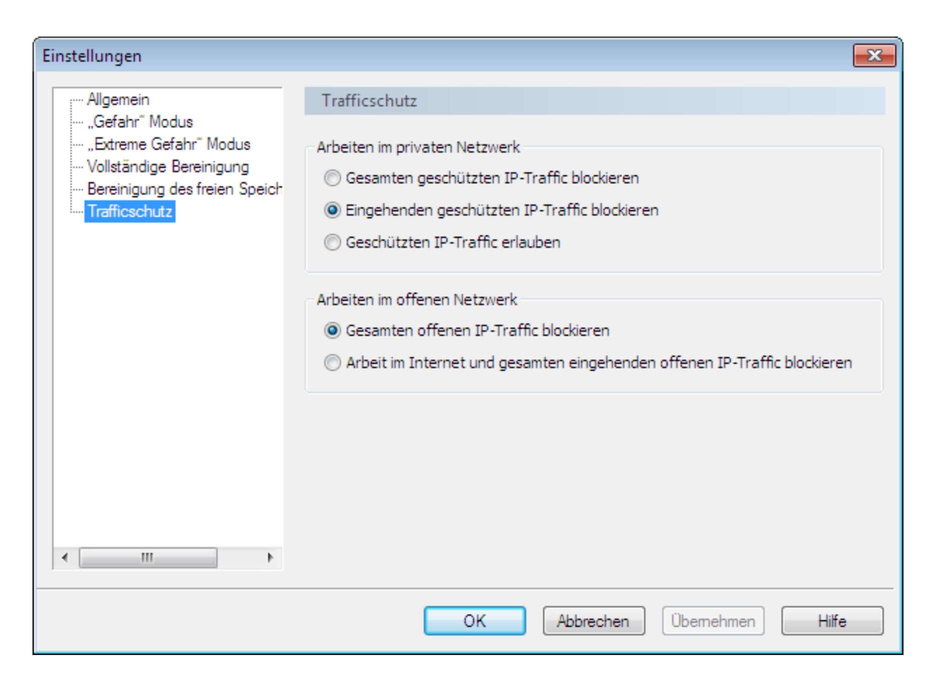
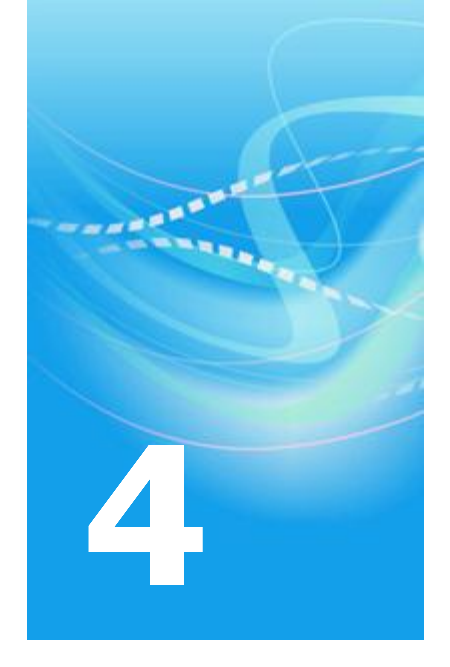


Abbildung 27: Konfiguration der Trafficschutz-Parameter

- Wählen Sie in Gruppe **Arbeit im privaten Netzwerk** den Zugangsmodus zum privaten Netzwerk, den Sie beim Arbeiten mit geschützten Containern verwenden möchten. Standardmäßig werden alle eingehenden verschlüsselten Verbindungen blockiert. Der sicherste Modus beim Arbeiten mit geschützten Containern ist der Modus, in welchem alle geschützten Verbindungen blockiert werden.
- Legen Sie in Gruppe **Arbeit im offenen Netzwerk** fest, ob die Kommunikation mit offenen Knoten beim Verwenden der geschützten Container blockiert werden soll. Standardmäßig werden alle Verbindungen mit offenen Netzwerken immer blockiert (Option Gesamten offenen Traffic blockieren). Es wird ausdrücklich davon abgeraten, den voreingestellten Wert zu ändern, da sogar das Erlauben ausschließlich ausgehender Verbindungen zum offenen Netzwerk beim Arbeiten mit sensiblen Daten in geschützten Containern potentiell gefährlich sein kann.

3 Klicken Sie auf **Übernehmen**.

Die eingestellten Parameter werden im Programm ViPNet Monitor angewendet. Details zur gemeinsamen Nutzung von ViPNet Monitor und ViPNet SafeDisk-V s. Abschnitt „Integration mit ViPNet SafeDisk-V“ im Dokument „ViPNet Client Monitor. Benutzerhandbuch“ bzw. „ViPNet Coordinator Monitor. Administratorhandbuch“.



Geschützte Daten exportieren und importieren

Wozu geschützte Daten exportiert und importiert werden können

Es kann manchmal erforderlich sein, mit geschützten Daten auch außerhalb des Büros zu arbeiten. Sie könnten zum Beispiel einen Bericht mit nach Hause nehmen, um ihn dort fertigzustellen. Dazu muss der Container mit privaten Daten zunächst von Ihrem Büro-Rechner auf Ihr privates Notebook übertragen werden. Das kann durch einen Export des ViPNet SafeDisk-V-Containers bewerkstelligt werden. Die Exportfunktionalität kann sowohl in der beschriebenen Situation als auch für die Erstellung von Sicherungskopien des Containers verwendet werden.

Nehmen wir an, dass Sie den Container auf Ihr Notebook exportiert und den Bericht beendet haben. Nun wollen Sie den Bericht an Ihren Vorgesetzten senden oder in ein Versionskontrollsystem hochladen. Nehmen wir zusätzlich an, dass Sie dies nur von Ihrem Büro-Rechner aus tun können (zum Beispiel aus Sicherheitsgründen). Um diese Aufgabe zu lösen, müssen Sie den fertigen Bericht zunächst von Ihrem Notebook auf den Büro-Computer übertragen. Ihr Bericht enthält sensible Daten, deswegen wollen Sie ihn nicht unter Verwendung konventioneller Methoden kopieren (mit Hilfe einer Diskette, eines USB-Sticks oder eines anderen mobilen Datenträgers). Der Bericht muss außerdem verschlüsselt bleiben. In diesem Fall können Sie das auf Ihrem Notebook installierte Programm ViPNet SafeDisk-V nutzen, um den Container mit dem Bericht zu exportieren. Anschließend können Sie mit Hilfe von ViPNet SafeDisk-V, das auf dem Büro-Rechner installiert ist, den Container importieren. Sie können die Importfunktionalität des Programms auch dazu verwenden, den Container aus einer Sicherungskopie wiederherzustellen.

Betrachten wir eine andere Situation. Sie fahren in den Urlaub, während Ihres Urlaubs müssen jedoch dringende Änderungen in ein von Ihnen erarbeitetes Projektkonzept eingebracht werden. Das Konzept enthält sensible Daten, deswegen kann es nicht ungeschützt übertragen werden. Sie können nun die Export- und Importmöglichkeiten von ViPNet SafeDisk-V nutzen, um dieses Problem zu lösen. Um das Dokument an eine Person zu übergeben, die während Ihrer Abwesenheit die notwendigen Änderungen vornehmen kann, können Sie den Container mit dem Bericht exportieren und ihn zusammen mit dem beim Export verwendeten Kennwort an diese Person weiterleiten. Ihr Vertreter kann den Container importieren, indem er das von Ihnen erhaltene Passwort benutzt. Nach Durchführung dieser Schritte kann Ihr Vertreter ungehindert mit den benötigten privaten Daten weiterarbeiten.

Nachfolgend sind Situationen aufgelistet, in denen die Import- und Exportfunktionalitäten von ViPNet SafeDisk-V von Nutzen sein könnten:

- Erstellung einer Sicherheitskopie oder Wiederherstellung privater Daten;

- Austausch geschützter Informationen zwischen zwei oder mehr Computern (sowohl über das Netzwerk als auch mit Hilfe mobiler Datenträger); auch wenn die Daten abgefangen werden, können sie dank der Verschlüsselung nicht angezeigt oder weiterverwendet werden;
- Weiterleitung geschützter Daten an einen anderen Mitarbeiter während Ihrer Abwesenheit im Büro.

Container exportieren

Beim Containerexport wird eine sogenannte Export-Datei des Containers erstellt. Sie sollten die Exportfunktionalität verwenden, wenn Sie folgende Aufgaben lösen wollen:

- Eine Sicherungskopie der im Container gespeicherten privaten Daten erstellen;
- vertrauliche Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen; private Daten während Ihrer Abwesenheit im Büro an einen Kollegen weiterleiten.

Zum Exportieren des Containers:

1. Wählen Sie im Programmfenster von ViPNet SafeDisk-V den Container aus, der exportiert werden soll. Wenn der Container eingebunden ist, trennen Sie ihn.
2. Wählen Sie im Menü **Container** den Befehl **Export**.
3. Geben Sie auf der ersten Seite des Assistenten **Container-Export** den Namen und den Pfad der Datei an, in welche der Container exportiert werden soll. Sie können die standardmäßig vorgegebenen Werte für Dateinamen und –pfad übernehmen oder auf die Schaltfläche ... klicken, um eine andere Datei auszuwählen. Klicken Sie anschließend auf **Weiter**.

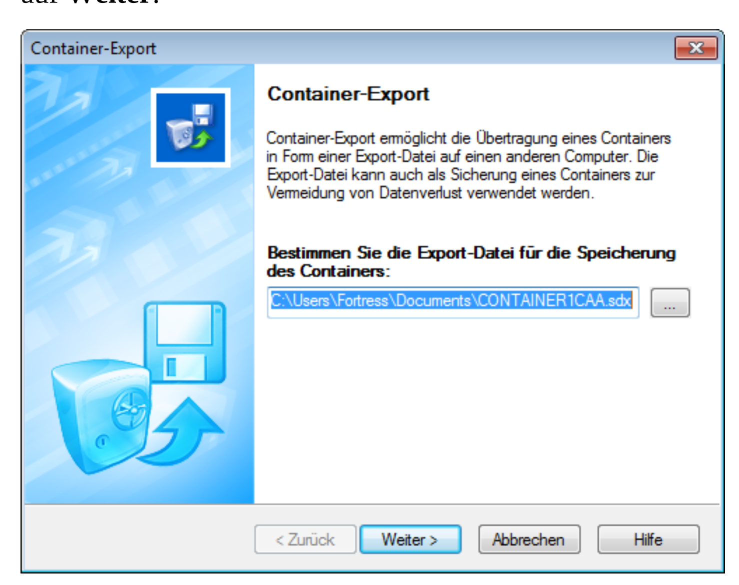


Abbildung 28: Assistent für den Container-Export



Tipp. Speichern Sie die Export-Datei des Containers aus Sicherheitsgründen nicht in demselben Ordner ab, in dem sich die Container-Datei befindet. Wir empfehlen, für die Speicherung der Container-Datei einen mobilen Datenträger zu verwenden.

4 Geben Sie auf der Seite **Passwort für die Export-Datei des Containers** ein Kennwort ein und wiederholen die Eingabe zur Bestätigung. Klicken Sie dann auf **Weiter**.

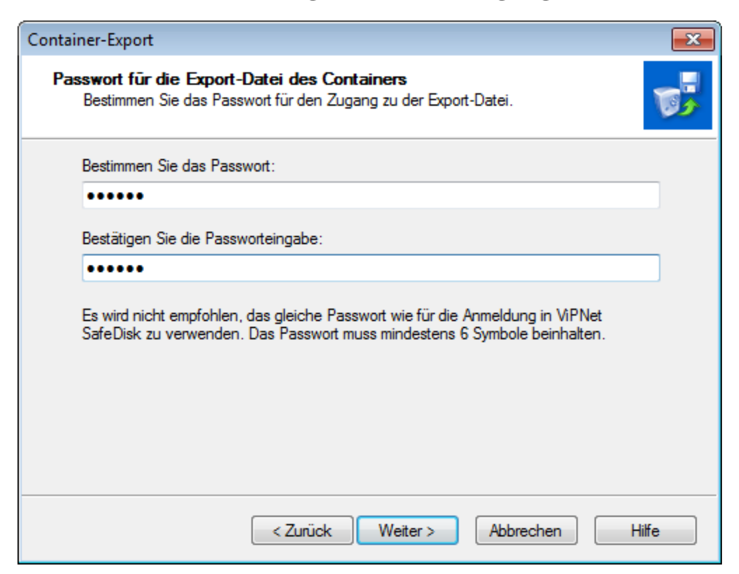


Abbildung 29: Kennwort für die Export-Datei des Containers eingeben

5 Definieren Sie auf der Seite **Container-Eigenschaften** die Parameter des zu exportierenden Containers:

- Wenn Sie verhindern wollen, dass der Inhalt des exportierten Containers verändert werden kann, aktivieren Sie das Kontrollkästchen **Den Container nur zum Lesen verwenden**.
- Wenn Sie möchten, dass der exportierte Container nach dem Import automatisch eingebunden wird, aktivieren Sie das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden**.

Klicken Sie auf **Weiter**.

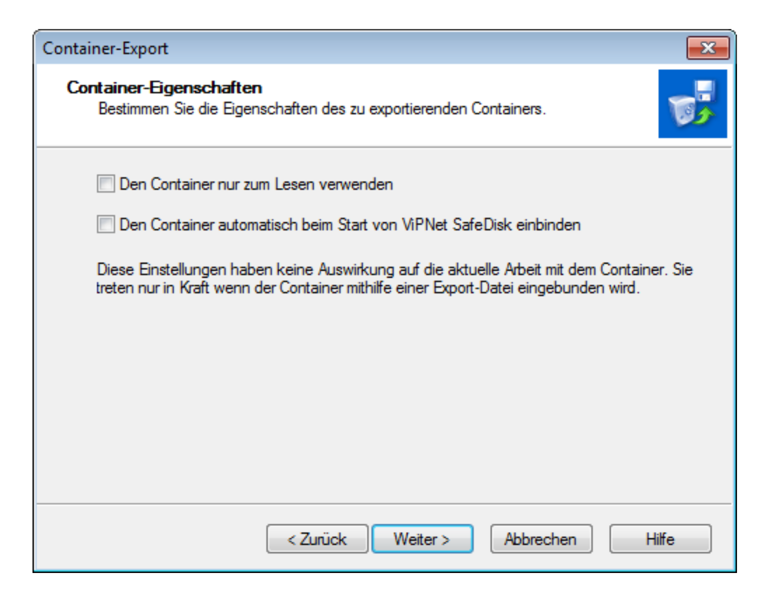


Abbildung 30: Container-Eigenschaften definieren

6 Klicken Sie auf der Seite **Abschluss des Container-Exports** auf die Schaltfläche **Fertig**.

Es wird die Export-Datei des Containers `*.sdx` angelegt (s. Exportdatei des Containers auf S. 144). Die Export-Datei beinhaltet die Container-Datei und eine Sicherungskopie der Containerschlüssel.

Sie können die neu erstellte Export-Datei des Containers mit Hilfe eines mobilen Datenträgers (CD, USB-Stick u. s. w.) oder über das Netzwerk (HTTP, FTP u. s. w.) auf einen anderen Computer übertragen.

Container importieren

Container aus einer Export-Datei importieren

Sie sollten den Container aus einer Export-Datei importieren, wenn Sie folgende Aufgaben lösen müssen:

- Geschützte Daten aus einer Sicherungskopie wiederherstellen (s. Wiederherstellen des Zugriffs auf die geschützten Daten auf S. 75).
- Mit geschützten Daten eines Kollegen während seiner Abwesenheit weiterarbeiten.

Damit der Container aus einer Export-Datei importiert werden kann, müssen Sie über folgende Objekte verfügen:

- Export-Datei des Containers (`*.sdx`);
- Kennwort, das beim Export des Containers verwendet wurde.

Führen Sie die folgenden Schritte aus, um den Container aus einer Export-Datei zu importieren:

1 Wählen Sie im Menü **Container** den Punkt **Import**. Der Assistent **Container-Import** wird gestartet.

2 Wählen Sie auf der Seite **Container-Import** die Option Datei und klicken auf **Weiter**.



Abbildung 31: Assistent für den Container-Import

3 Klicken Sie auf der Seite **Zugangspasswort** auf die Schaltfläche ... und geben Sie den Pfad zur Export-Datei des Containers an. Wählen Sie in der Liste **Dateityp** den Eintrag **Container-Export (*.sdx)** aus, um die Dateisuche zu beschleunigen.

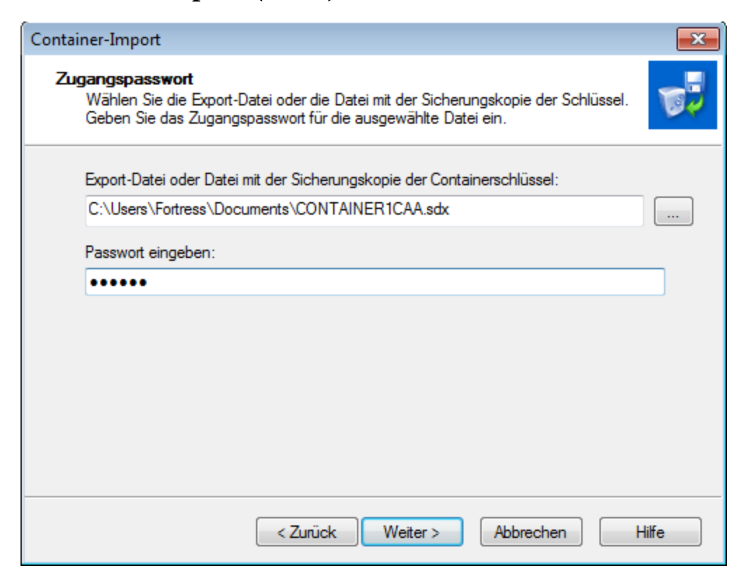


Abbildung 32: Zugangskennwort eingeben

4 Geben Sie im Feld **Passwort eingeben** das Kennwort ein, das beim Export des Containers verwendet wurde. Klicken Sie anschließend auf **Weiter**.

5 Geben Sie auf der Seite **Container-Datei** den Namen und den Pfad der Datei des Containers an, in welchem der zu importierende Container untergebracht werden soll.

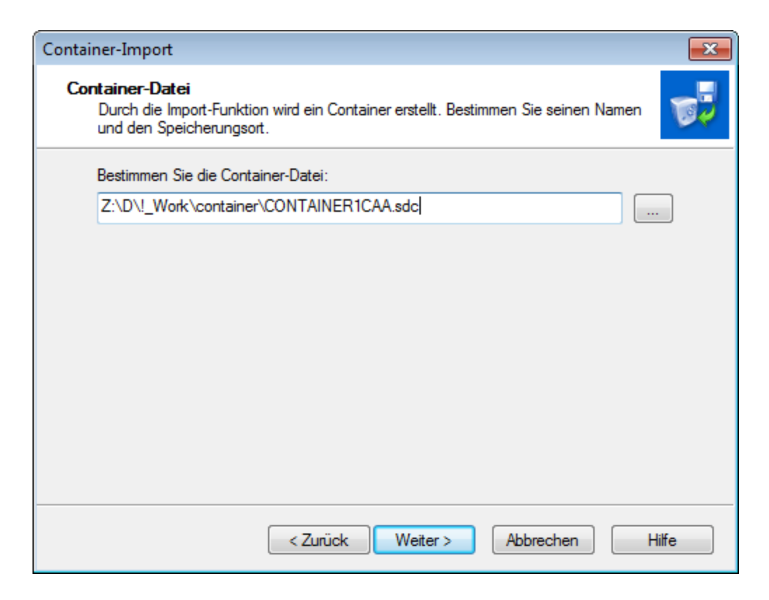


Abbildung 33: Speicherort des zu importierenden Containers bestimmen

6 Wenn die beim letzten Schritt definierte Container-Datei bereits existiert, geben Sie auf der Seite **Der Container existiert bereits** an, ob der bestehende Container vollständig ersetzt werden soll, oder ob nur die Schlüssel des bestehenden Containers ersetzt werden sollen.

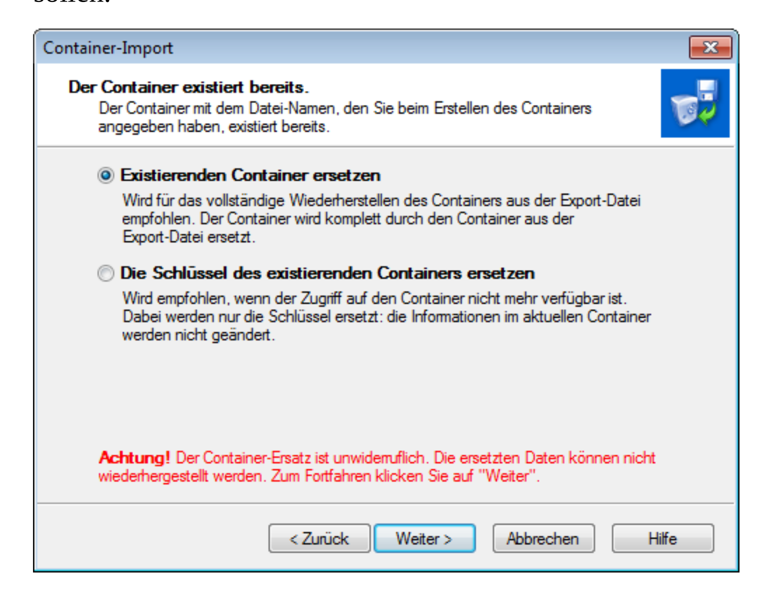


Abbildung 34: Bestimmen, ob der Container ersetzt wird

7 Wenn Sie nicht wollen, dass der Container sofort nach dem Import in einem separaten Fenster geöffnet wird, deaktivieren Sie im Fenster **Abschluss des Container-Imports** das Kontrollkästchen **Container einbinden**.

Klicken Sie auf **Fertig**.

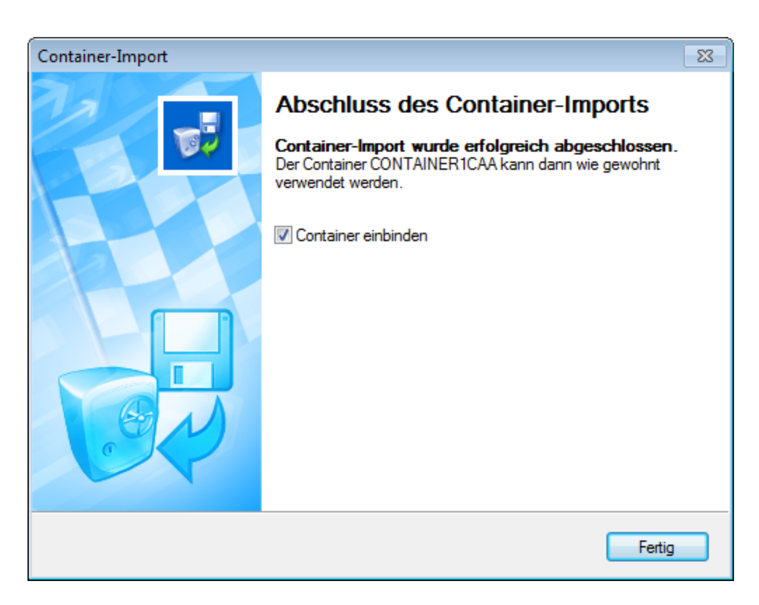


Abbildung 35: Abschluss des Container-Imports

Es wird ein neuer Container angelegt, der eine Kopie des importierten Containers darstellt. Der neue Container wird im Hauptfenster von ViPNet SafeDisk-V angezeigt.

Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren

In folgenden Fällen sollten Sie den Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren:

- Es wurden Schlüssel beschädigt, mit denen der Container verschlüsselt wurde. Wenn der Container selbst intakt ist, können Sie mit Hilfe der Sicherungskopie der Containerschlüssel den Zugang zu geschützten Daten wiederherstellen (s. Wiederherstellen des Zugriffs auf die geschützten Daten auf S. 75).
- Sie erhalten die Container-Datei (jedoch nicht die Export-Datei des Containers) sowie eine Sicherungskopie der Schlüssel dieses Containers. Sie wollen den Container einbinden, um Zugriff auf die im Container gespeicherten privaten Daten zu erhalten.

Führen Sie die folgenden Schritte aus, um den Container mit Hilfe der Sicherungskopie seiner Schlüssel zu importieren:

1. Wählen Sie im Menü **Container** den Punkt **Import**. Es wird der Assistent **Container-Import** gestartet.
2. Gehen Sie auf der Seite **Container-Import** (s. Abbildung auf S. 69) wie folgt vor:

- Wenn die Sicherungskopie der Containerschlüssel in einer Datei auf dem Computer gespeichert ist, führen Sie die folgenden Schritte aus:
  - Wählen Sie die Option **Datei** und klicken Sie auf **Weiter**.
  - Klicken Sie auf der Seite **Zugangspasswort** (s. Abbildung auf S. 69) auf die Schaltfläche ... und geben den Pfad zur Datei mit der Sicherungskopie der Containerschlüssel an. Wählen Sie in der Liste **Dateityp** den Eintrag **Sicherungskopie der Containerschlüssel (*.sde)** aus, um die Dateisuche zu beschleunigen.
  - Geben Sie im Feld **Passwort eingeben** das Kennwort ein, das beim Erstellen der Sicherungskopie der Containerschlüssel verwendet wurde. Klicken Sie anschließend auf **Weiter**.
- Wenn die Sicherungskopie der Containerschlüssel auf einem externen Gerät gespeichert ist, führen Sie die folgenden Schritte aus:
  - Wählen Sie die Option **Externes Authentisierungsgerät** und klicken auf **Weiter**. Es wird die Seite **Externes Authentisierungsgerät auswählen** eingeblendet.

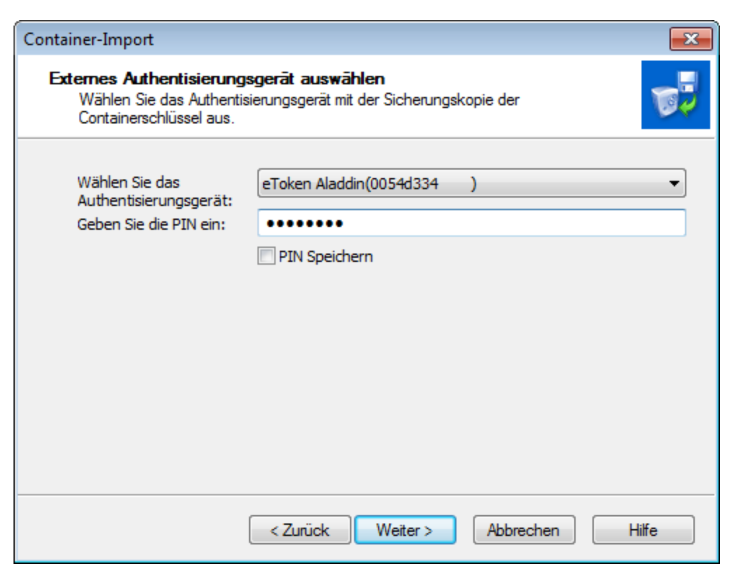


Abbildung 36: Externes Gerät auswählen

  - Stellen Sie sicher, dass das externe Gerät mit der entsprechenden Leseeinrichtung verbunden ist.
  - Wählen Sie in der Liste **Wählen Sie das Authentisierungsgerät** das benötigte Gerät aus (wenn es nicht bereits automatisch ausgewählt wurde).



Hinweis. Die Sicherungskopie der Containerschlüssel (s. Sicherungskopie der Containerschlüssel erstellen auf S. 39) muss vorher bereits auf dem ausgewählten Gerät gespeichert worden sein.

- Geben Sie im Feld **Geben Sie die PIN ein** den Zugangscode für das Gerät ein. Um die PIN zu speichern, aktivieren Sie das entsprechende Kontrollkästchen.
- Klicken Sie auf **Weiter**. Es wird die Seite **Sicherungskopie der Containerschlüssel auswählen** eingeblendet.

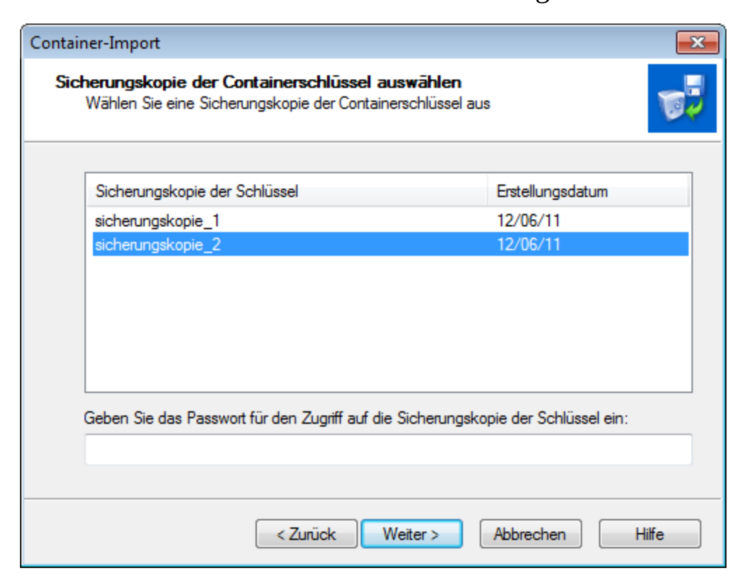


Abbildung 37: Sicherungskopie auswählen

- Wählen Sie aus der Liste der Sicherungskopien diejenige aus, die Sie für den Container-Import verwenden möchten.
- Geben Sie das Zugangspasswort für die gewählte Sicherungskopie der Schlüssel ein und klicken auf **Weiter**.

3 Wenn sich die Sicherungskopie der Containerschlüssel und die Container-Datei in unterschiedlichen Ordnern befinden, klicken Sie auf der Seite **Container-Datei** auf die Schaltfläche ... und geben Sie den Pfad zur Container-Datei an.

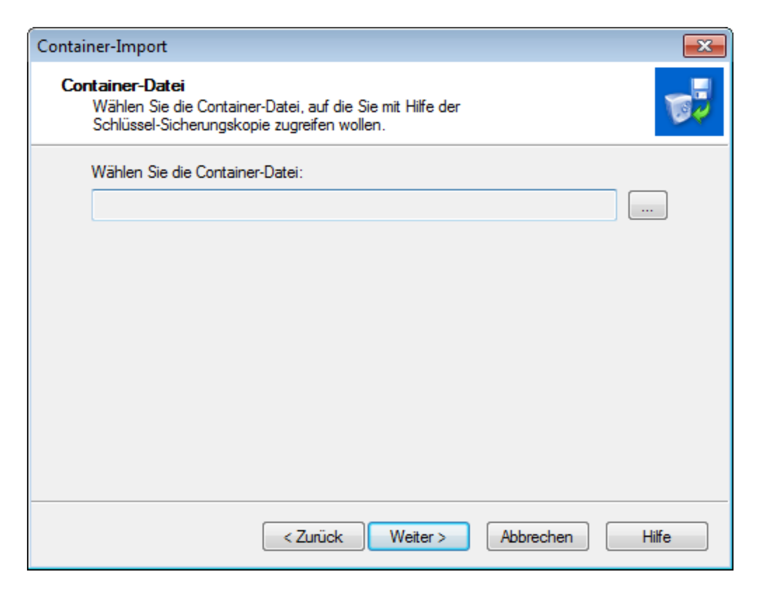


Abbildung 38: Pfad zur Container-Datei definieren

4 Wenn Sie nicht wollen, dass der Container sofort nach dem Import in einem separaten Fenster geöffnet wird, deaktivieren Sie auf der Seite **Abschluss des Container-Imports (s. Abbildung auf S. 71) das Kontrollkästchen Container einbinden.**

Klicken Sie auf **Fertig**.

Nach Abschluss des Assistenten sieht die Situation folgendermaßen aus:

- wenn Sie den Zugang zu einem Container wiederherstellen wollten, dessen Schlüssel beschädigt waren, wird der Zugang nun wieder hergestellt;
- wenn Sie die Sicherungskopie der Schlüssel verwendet haben, um eine Container-Datei zu importieren, wird der Container nun importiert, und Sie können beginnen, mit den im Container enthaltenen privaten Daten zu arbeiten.



Hinweis. Wenn Sie den Container aus einer Export-Datei importieren, dann wird ein neuer Container angelegt, der eine Kopie des importierten Containers darstellt.

Wenn Sie den Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren, dann erhalten Sie unmittelbar den Zugang zum importierten Container (eine Kopie wird nicht angelegt).



Wiederherstellen des Zugriffs auf die geschützten Daten

Warum Daten wiederhergestellt werden müssen

Daten sind oft unbezahlbar. Wenn wichtige Informationen verloren gehen oder in die Hände von Übeltätern gelangen, kann das sowohl zu kleinen Unannehmlichkeiten als auch zu riesigen finanziellen Verlusten führen. Seit Computer aus dem täglichen Geschäftsleben nicht mehr wegzudenken sind, haben alle Organisationen das Bestreben, ihre Daten auf bestmöglichen Weg zu schützen.

Die regelmäßige Erstellung von Sicherungskopien ist eine der am weitesten verbreiteten Methoden, mit deren Hilfe Daten geschützt und im Notfall schnell wiederhergestellt werden können. Wenn mit der aktuellen Version Ihrer Daten etwas geschehen sollte, können Sie die Daten aus der letzten Sicherungskopie wiederherstellen. Auch wenn einige unwesentliche Änderungen verlorengehen, wird der grundlegende Teil der Daten erfolgreich wiederhergestellt, und Sie können schnell zum Normalbetrieb zurückkehren.

Sie können ViPNet SafeDisk-V für den Schutz Ihrer Daten verwenden, indem Sie regelmäßig Sicherungskopien aller Container, einiger ausgewählter Container oder nur der Containerschlüssel erstellen.

Geschützte Daten wiederherstellen: praktische Hinweise

Damit ein höheres Sicherheitsniveau gewährleistet werden kann, bietet ViPNet SafeDisk-V mehrere Methoden zur Wiederherstellung vertraulicher Daten an. Sie helfen dabei, bei Auftreten etwaiger Störungen die Arbeit mit den geschützten Daten schnell wieder fortzusetzen.

In der nachfolgenden Tabelle sind einige Problemfälle aufgelistet, die im Zuge der Verwendung privater Daten auftreten können. Daneben sind Empfehlungen für eine effektive Lösung der Probleme angegeben.

Problem	Lösung
Der Zugang kann nicht für alle Container hergestellt werden.	Damit der Zugang wieder gewährleistet werden kann, sollte die Konfiguration wiederhergestellt werden (s. Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen auf S. 79). Dazu muss eine rechtzeitig erstellte Sicherungskopie der Konfiguration zur Verfügung stehen, und die Container-Dateien dürfen nicht beschädigt sein.
Der Zugriff auf einen oder mehrere Container ist nicht möglich.	In diesem Fall kann der Zugang zum Container mit Hilfe einer Sicherungskopie seiner Schlüssel wieder hergerichtet werden (s. Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren auf S. 71). Die Container-Datei darf dabei nicht beschädigt sein.
Die Container-Datei ist beschädigt.	Zum Wiederherstellen der Daten sollten Sie den Container aus einer zuvor erstellten Export-Datei des Containers importieren (s. Container aus einer Export-Datei importieren auf S. 68).
Ein Festplattenfehler ist aufgetreten. Nur die Sicherungskopien der Containerschlüssel sind erhalten geblieben.	Die geschützten Daten können nicht wiederhergestellt werden, wenn die Container-Datei beschädigt ist und gleichzeitig keine Export-Datei dieses Containers zur Verfügung steht. Sie können versuchen, die Container-Datei auf der beschädigten Festplatte wiederherzustellen. Wenn das gelingt, können Sie den Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren. Der beste Weg, ähnliche Probleme zu vermeiden, ist die regelmäßige Erstellung von Sicherungskopien der Container-Datei (s. Container exportieren auf S. 65).
Ein Festplattenfehler ist aufgetreten. Nur	Wenn die Container-Datei intakt, die Sicherungskopie der Containerschlüssel jedoch beschädigt ist, können private Daten

Problem	Lösung
die Container-Datei ist erhalten geblieben.	nicht wiederhergestellt werden. Versuchen Sie, die Sicherungskopie der Containerschlüssel auf der beschädigten Festplatte wiederherzustellen (vorausgesetzt, die Sicherungskopie wurde rechtzeitig erstellt). Wenn das gelingt, können Sie den Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren Der beste Weg, ähnliche Probleme zu vermeiden, ist die regelmäßige Erstellung von Sicherungskopien der Container-Datei (s. Container exportieren auf S. 65).



Achtung! Damit der Arbeitsablauf bei der Erstellung von Sicherungskopien und bei der Wiederherstellung von Daten vereinfacht werden kann, empfehlen wir, regelmäßig folgende Aktionen durchzuführen:

- Export-Dateien des Containers erstellen;
- Sicherungskopien der Containerschlüssel erstellen;
- Sicherungskopien der Konfiguration erstellen.

Wenn Sie sich an diese Empfehlungen halten, werden Sie Ihre vertraulichen Daten im Fall von unvorhersehbaren Störungen leicht wiederherstellen und den Zeitaufwand für die Wiederherstellung von Änderungen, die nach der letzten Sicherung vorgenommen wurden, deutlich reduzieren können.

Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen

Wenn der Zugang zu keinem Ihrer Containern mehr möglich ist, besteht der beste Weg zum Wiederherstellen der Daten in einer **Wiederherstellung der Konfiguration**.

Damit eine bestimmte Konfiguration wiederhergestellt werden kann, muss eine Sicherungskopie dieser Konfiguration rechtzeitig angelegt werden. Sie können so viele Sicherungskopien erstellen wie nötig sind.

Die Sicherungskopien der ViPNet SafeDisk-V-Konfiguration werden außerdem automatisch erstellt, wenn Sie sich im Programm abmelden oder eine Konfiguration wiederherstellen.

Sicherungskopie der Konfiguration erstellen

Eine Sicherungskopie der Konfiguration wird erstellt, um nachträglich die aktuelle Konfiguration des Programms wieder herstellen zu können.



Achtung! Wenn mehrere Benutzer mit einer Instanz von ViPNet SafeDisk-V arbeiten, muss jeder von ihnen seine eigenen Sicherungskopien der Konfiguration anlegen. Jeder Benutzer kann nur auf die von ihm selbst erstellten Sicherungskopien zugreifen.

Zum Erstellen einer Sicherungskopie der Konfiguration:

1. Trennen Sie alle eigebundenen Container.
2. Wählen Sie im Menü **SafeDisk** den Befehl **Wiederherstellung der Konfiguration**. Es wird der Assistent **Wiederherstellen der ViPNet SafeDisk-V Konfiguration** gestartet.
3. Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk-V Konfiguration** das Kontrollkätschen **Sicherungskopie der aktuellen Konfiguration erstellen** und klicken Sie auf **Weiter**.



Abbildung 39: Assistent zum Wiederherstellen einer ViPNet SafeDisk-V-Konfiguration

4 Geben Sie auf der Seite **Erstellen der Sicherungskopie** im Feld **Kommentar** eine Beschreibung der Konfiguration ein. Dies ist nicht obligatorisch, wird aber helfen, die gewünschte Sicherungskopie in der Liste zu finden. Der Kommentar darf maximal 200 Zeichen lang sein.

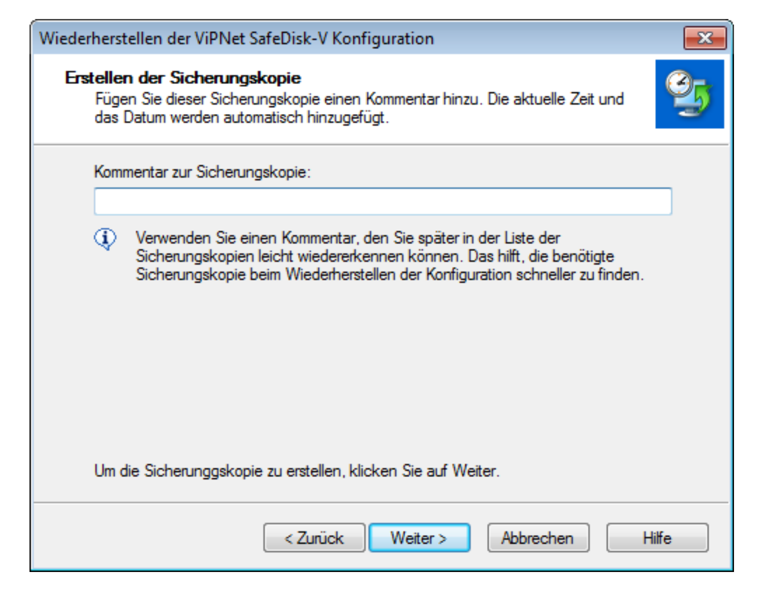


Abbildung 40: Sicherungskopie der Konfiguration erstellen

5 Klicken Sie auf **Weiter**. Die Sicherungskopie der Konfiguration wird nun erstellt.

Die erstellte Sicherungskopie wird im Unterordner `\Restore` des Installationsordner des Programms gespeichert.

6 Klicken Sie auf der Seite **Abschluss der Erstellung der Sicherungskopie** auf **Fertig**, um den Assistenten abzuschließen.

7 Wenn Sie die Arbeit mit Sicherungskopien fortsetzen möchten, klicken Sie auf **Zum Anfang**.

Liste von Sicherungskopien der Konfiguration editieren

Sie können Ihre Liste der Sicherungskopien der Konfiguration editieren: Sicherungskopien löschen oder Kommentare bearbeiten.

Zum Editieren der Liste von Sicherungskopien der Konfiguration:

1 Trennen Sie alle Container.

2 Wählen Sie im Menü **SafeDisk** den Befehl **Wiederherstellung** der Konfiguration. Es wird der Assistent **Wiederherstellen der ViPNet SafeDisk-V Konfiguration** gestartet.

3 Wählen Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk-V Konfiguration** die Option **Die Liste der Sicherungskopien ändern** und klicken anschließend auf **Weiter**.

4 Wählen Sie auf der Seite **Ändern der Liste der Sicherungskopien** die Sicherungskopie aus, die Sie bearbeiten wollen. Wenn Sie den Kommentar zur Sicherungskopie ändern möchten, klicken Sie auf die Schaltfläche **Kommentar ändern**. Wenn Sie die Sicherungskopie löschen möchten, klicken Sie auf **Löschen**.

   Die Sicherungskopien der Konfiguration werden automatisch nach Erstellungsdatum oder nach Kommentaren sortiert. Zum Ändern der Sortierreihenfolge klicken Sie auf die Spaltenüberschrift **Erstellungszeit und -Datum** oder auf **Kommentar**.

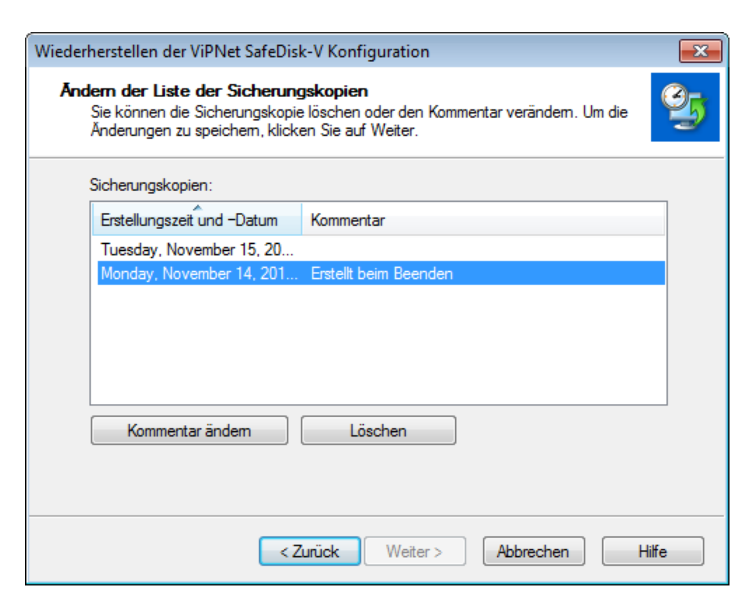


Abbildung 41: Liste der Sicherungskopien bearbeiten

5 Klicken Sie auf **Weiter**, um die Bearbeitung abzuschließen.

6 Klicken Sie auf der Seite **Bearbeitung der Liste der Sicherungskopien abschließen** auf **Fertig**, um den Assistenten abzuschließen.

Wenn Sie die Arbeit mit Sicherungskopien fortsetzen möchten, klicken Sie auf **Zum Anfang**.

Konfiguration wiederherstellen

Um die Konfiguration von ViPNet SafeDisk-V aus einer Sicherungskopie wiederherzustellen, führen Sie die folgenden Schritte durch:

1 Trennen Sie alle Container.

2 Wählen Sie im Menü **SafeDisk** den Befehl **Wiederherstellung der Konfiguration**. Es wird der Assistent **Wiederherstellen der ViPNet SafeDisk-V Konfiguration** gestartet.

3 Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk-V Konfiguration** die Option **ViPNet SafeDisk-V Konfiguration wiederherstellen** und klicken anschließend auf **Weiter**.

Wenn dieser Option nicht verfügbar ist, bedeutet das, dass keine Sicherungskopien der Konfiguration erstellt wurden. In diesem Fall kann der Zugang zu diesem Container mit Hilfe der Importfunktionalität unter Verwendung einer Sicherungskopie seiner Schlüssel oder einer Export-Datei dieses Containers wiederhergestellt werden.

4 Auf der Seite **Auswahl der Sicherungskopie** wird eine Liste der gespeicherten Sicherungskopien angezeigt.

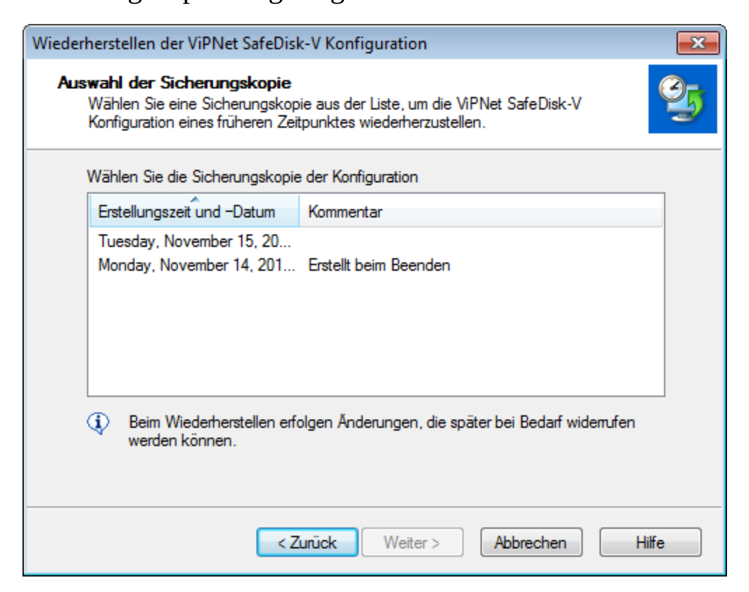


Abbildung 42: Sicherungskopie auswählen

Die Sicherungskopien der Konfiguration werden automatisch nach Erstellungszeit und -datum sortiert. Klicken Sie zum Ändern der Sortierreihenfolge auf die Spaltenüberschrift **Erstellungsdatum/-zeit** oder **Kommentar**.

5 Klicken Sie auf der Seite **Abschluss der Wiederherstellung der ViPNet SafeDisk-V-Konfiguration** auf die Schaltfläche **Fertig**, um den Assistenten abzuschließen.

Es wird der Vorgang der Wiederherstellung der gewählten Konfiguration von ViPNet SafeDisk-V gestartet.

Wenn Sie die Arbeit mit Sicherungskopien fortsetzen möchten, klicken Sie auf **Zum Anfang**.



Hinweis. Die letzte Wiederherstellung kann immer rückgängig gemacht werden. Außerdem kann die Wiederherstellung aus einer anderen Sicherungskopie eingeleitet werden, indem Sie zur ersten Seite des Assistenten zurückkehren. Wenn der Assistent bereits beendet wurde, starten Sie ihn neu.

Wenn Sie nach der Wiederherstellung der Konfiguration immer noch kein Zugriff auf die Container haben, sind möglicherweise die Containerdateien beschädigt. In diesem Fall versuchen Sie jeden einzelnen Container aus der entsprechenden Export-Datei separat zu importieren. Dazu sollten Sie über bereits früher erstellte Export-Dateien der Container verfügen (s. Container exportieren auf S. 65).

Letzte Wiederherstellung der Konfiguration rückgängig machen

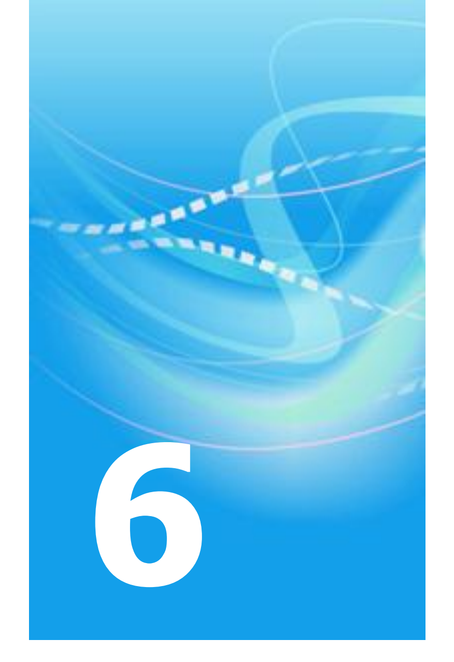
Wenn die Wiederherstellung der Konfiguration das Problem nicht gelöst hat, können Sie zu einer früheren Konfiguration zurückkehren. Dazu müssen Sie die zuletzt durchgeführte Wiederherstellung der Konfiguration widerrufen.

Damit die letzte Wiederherstellung der Konfiguration rückgängig gemacht wird:

1. Trennen Sie alle Container.
2. Wählen Sie im Fenster des Programms ViPNet SafeDisk im Menü **SafeDisk** den Befehl **Wiederherstellung der Konfiguration**. Es wird der Assistent **Widerherstellung der ViPNet SafeDisk Konfiguration**.
3. Wählen Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk Konfiguration** die Option **Die letzte Wiederherstellung widerrufen** und klicken Sie anschließend auf **Weiter**.

   Der Widerruf der letzten Wiederherstellung der Konfiguration wird gestartet.
4. Klicken Sie auf der Seite **Widerruf der letzten Konfigurationswiederherstellung abschließen** auf die Schaltfläche **Fertig**, um den Assistenten abzuschließen.

   Wenn Sie die Arbeit mit Sicherungskopien fortsetzen möchten, klicken Sie auf **Zum Anfang**.



Gemeinsame Nutzung von ViPNet SafeDisk-V

Zugriff auf die Container für mehrere Benutzer einrichten

Mit Hilfe von ViPNet SafeDisk-V können Sie den Zugang zu Ihren Containern auch anderen Benutzern zur Verfügung stellen, um gemeinsam mit geschützten Daten, die in diesen Containern gespeichert sind, arbeiten zu können.

Der allgemeine Zugang zu Containern kann auf zwei Arten eingerichtet werden:

1. Den Zugang zu Ihrem Container einem oder mehreren Benutzern auf demselben Computer oder auf unterschiedlichen Computern zur Verfügung stellen. Dazu müssen Sie entweder eine Sicherungskopie der Containerschlüssel an die Benutzer weiterleiten (falls diese Benutzer den gleichen Rechner verwenden wie Sie), oder die Container-Datei selbst mitsamt einer Sicherungskopie der Schlüssel dieses Containern bereitstellen (wenn diese Benutzer andere Rechner verwenden). Bei dieser Art des allgemeinen Containerzugangs ist die gleichzeitige gemeinsame Arbeit an vertraulichen Daten, die im entsprechenden Container gespeichert sind, nicht möglich. Auch wenn sich der Container auf einem Netzlaufwerk befindet, können mehrere Benutzer nicht gleichzeitig mit dem Container arbeiten.
2. Den allgemeinen Zugang zu Ihren Containern über das Netzwerk einrichten. Bei dieser Art des Containerzugangs gewähren Sie den Zugang nicht zur Container-Datei selbst, sondern zum Laufwerk, das dem eingebundenen Container unter Windows entspricht. Sie erhalten dadurch die volle Kontrolle darüber, wer und wann auf Ihre geschützten Daten zugreifen darf.

Der erste Ansatz eignet sich gut für Situationen, in welchen ein Kollege Ihre Arbeit fortsetzen soll, weil Sie zum Beispiel in Urlaub gehen. In diesem Fall muss zunächst eine Sicherungskopie der Containerschlüssel an diesen Kollegen weitergeleitet werden. Er muss sich in ViPNet SafeDisk-V mit seinem Kennwort anmelden und den Container mit Hilfe der Sicherungskopie der Schlüssel importieren. Wenn dieser Mitarbeiter keinen Zugang zu Ihrem Rechner hat, müssen Sie ihm die Container-Datei und eine Sicherungskopie der Schlüssel dieses Containers übergeben.

Der zweite Ansatz scheint passend, wenn die gemeinsame Arbeit an sensiblen Dokumenten im Vordergrund steht. Nehmen wir an, Sie erstellen ein Projektkonzept. Nun wollen Sie dieses Konzept mit den Teamkollegen besprechen und mögliche Verbesserungen in das entsprechende Dokument eintragen lassen. Dazu muss der Container, der das Konzept enthält, zuerst

eingebunden, und der Zugang zum Laufwerk, das diesem Container unter Windows zugeordnet ist, für andere Benutzer freigegeben werden.

Abgrenzung des Containerzugangs

Die Abgrenzung des Containerzugangs kann grundsätzlich in zwei Typen unterteilt werden:

- Zugangsbeschränkungen in Abhängigkeit vom Dateisystem, in dem der Container formatiert wurde;
- Zugangsbeschränkungen in Abhängigkeit vom verwendeten Betriebssystem.

Die einzelnen Abhängigkeiten bei den Zugangsbeschränkungen sind in der unteren Tabelle aufgeführt.

Tabelle 4. Abgrenzung des Containerzugangs

Verwendetes Betriebssystem	**Dateisystem des Containers**	
	NTFS	**FAT / FAT32**
Microsoft Windows XP SP3 (32-Bit)/Server 2003 (32/64-Bit)	Wenn beim Einbinden des Containers das Kontrollkästchen **Exklusiver Zugriff** aktiviert wurde, dann werden die Berechtigungen für das Laufwerk, das dem Container entspricht, so festgelegt, dass mit Ausnahme des Benutzers, der den Container eingebunden hat, niemand sonst irgendwelche Aktionen in Bezug auf dieses Laufwerk ausführen kann, unabhängig davon, welche Berechtigungen für dieses Laufwerk im Betriebssystem festgesetzt wurden. Ebenso wird es nicht möglich sein, einen Netzwerkzugang zu diesem Laufwerk einzurichten. Einerseits kann dadurch die Sicherheit der Arbeit in Situationen, wenn mehrere Benutzer gleichzeitig auf einem Computer arbeiten können, wesentlich erhöht werden. Andererseits werden dadurch die Möglichkeiten zur gemeinsamen Arbeit mehrerer Benutzer mit einem Container eingeschränkt. Wenn beim Einbinden des Containers das Kontrollkästchen **Exklusiver Zugriff** nicht aktiviert wurde, dann werden Berechtigungen wirksam, die für die Betriebssysteme Vista SP2 (32/64-Bit)/Server 2008 (32/64-Bit)/Windows 7 (32/64-Bit) gelten und weiter unten beschrieben sind.	
	Beim Einbinden des Containers werden	Vollständiger Zugriff aller

Verwendetes	Dateisystem des Containers	
Vista SP2 (32/64-Bit)/Server 2008 (32/64-Bit)/Windows 7 (32/64-Bit)	die Berechtigungen so festgelegt, dass nur der Benutzer, der den Container im Programm ViPNet SafeDisk eingebunden hat, den vollen Zugriff auf das Laufwerk, das dem Container entspricht, besitzt. Beim Bereitstellen des öffentlichen Zugangs zum Container über das Netzwerk kann der Zugang der Benutzer zum Laufwerk, das dem Container entspricht, mit Hilfe der Betriebssystem-Werkzeuge erlaubt oder blockiert werden.	Benutzer auf die Container.

Containerzugang für einen oder mehrere Benutzer auf demselben oder auf unterschiedlichen Computern bereitstellen

Zum Einrichten des Containerzugangs für andere Benutzer:

1. Wenn eine Sicherungskopie der Containerschlüssel noch nicht angelegt wurde, erstellen Sie diese (s. Sicherungskopie der Containerschlüssel erstellen auf S. 39).
2. Leiten Sie die Sicherungskopie der Containerschlüssel (Datei *.sde) und das Kennwort, das beim Anlegen der Sicherungskopie verwendet wurde, an den Benutzer weiter, dem Sie den Zugang zum Container gewähren möchten.
3. Wenn der Zugang für einen Benutzer eingerichtet werden soll, der auf einem anderen Computer arbeitet, übergeben Sie ihm auch die Container-Datei (*.sdc).



Achtung! Wenn Sie mit Hilfe einer Sicherungskopie der Schlüssel einem anderen Benutzer den Zugang zum Container auf Ihrem Rechner gewährt und später die Schlüssel dieses Containers aktualisiert haben (s. Containerschlüssel aktualisieren auf S. 54), dann verliert der andere Benutzer die Zugangsmöglichkeit wieder. Um die Arbeit mit Ihrem Container fortsetzen zu können, muss dieser Benutzer den Container mit Hilfe einer Sicherungskopie der neuen Schlüssel nochmals importieren (s. Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren auf S. 71).

Wenn ein anderer Benutzer den Zugang zu seinem Container bereitstellt:

1. Starten Sie ViPNet SafeDisk-V.
2. Wählen Sie im Menü **Container** den Befehl **Import**. Es wird der Assistent **Container-Import** gestartet.
3. Führen Sie den Import des Containers mit Hilfe einer Sicherungskopie seiner Schlüssel durch (s. Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren auf S. 71).

Nach Abschluss des Importvorgangs verfügen beide Benutzer über den Zugang zum Container. Wenn Sie die Sicherungskopie der Containerschlüssel an mehrere Benutzer übergeben haben, sind diese Benutzer nun ebenfalls imstande, auf den Container zuzugreifen. Es kann aber jeweils nur ein Benutzer zur gleichen Zeit mit dem Container arbeiten.

Netzwerkzugang auf einen Container für mehrere Benutzer ermöglichen

Damit mehrere Benutzer gleichzeitig oder anwechselnd mit geschützten Daten in Ihrem Container arbeiten können, muss das Laufwerk, das den Container im Betriebssystem Windows repräsentiert, für diese Benutzer freigegeben werden. Dadurch können Sie auch Benutzern, die ViPNet SafeDisk-V nicht auf ihren Rechnern installiert haben, den Zugriff auf die Daten in Ihrem Container erlauben.



Achtung! Seien Sie vorsichtig, wenn Sie den Containerzugang über das Netzwerk bereitstellen. Es werden auch Benutzer auf geschützte Daten in diesem Container zugreifen können, die ViPNet SafeDisk-V nicht installiert haben.



Hinweis. Beim Einbinden des Containers werden in den Betriebssystemen Windows Vista und höher die Rechte für die Ausführung der Dateien, die im Container enthalten sind, nur demjenigen Benutzer zugeteilt, unter dessen Konto der Container eingebunden wurde. Einige Programme dürfen nur mit Administratorrechten gestartet werden. Wenn demnach der Benutzer, der den Container eingebunden hat, über keine Administratorrechte verfügt, werden diese Programme nicht gestartet werden können.

Beim Auftreten einer solchen Situation wird empfohlen, die auszuführenden Dateien als Administrator zu starten oder dem Benutzer, der den Container einbindet, Administratorrechte zu erteilen.

Damit mehrere Benutzer gleichzeitig mit Ihren geschützten Daten arbeiten können, gehen Sie wie folgt vor:

1 Wählen Sie im Hauptfenster von ViPNet SafeDisk-V den Container aus, der für den allgemeinen Zugang bereitgestellt werden soll.

2 Binden Sie den gewählten Container ein, falls er noch nicht eingebunden ist.

3 Öffnen Sie den Ordner **Arbeitsplatz** (über das Menü **Start** oder durch Anklicken des entsprechenden Symbols auf dem **Desktop**), klicken Sie mit der rechten Maustaste auf das Laufwerk, das dem gewählten Container entspricht, und wählen Sie im Kontextmenü den Eintrag **Freigabe und Sicherheit**. Es wird das Fenster **Eigenschaften von Lokaler Datenträger** eingeblendet.

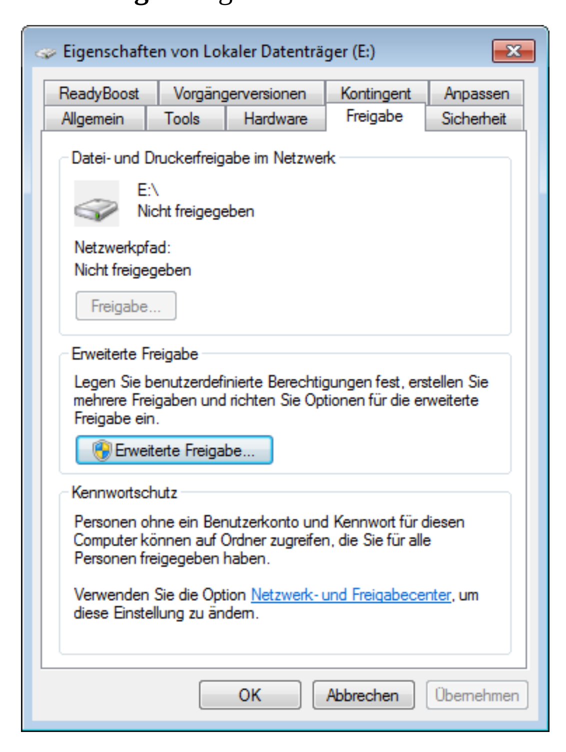


Abbildung 43: Fenster mit Eigenschaften des lokalen Laufwerks

4 **In Windows Vista/Server 2008/Windows 7:**

- Klicken Sie im Fenster **Eigenschaften von Lokaler Datenträger** in der Registerkarte **Freigabe** auf die Schaltfläche **Erweiterte Freigabe**.
- Aktivieren Sie im Fenster **Erweiterte Freigabe** das Kontrollkästchen **Diesen Ordner freigeben**. Geben Sie einen Namen für das freigegebene Objekt und die maximal zulässige Anzahl an Benutzern, die gleichzeitig darauf zugreifen können, an. Ebenso können Sie Zugriffsberechtigungen definieren (Schaltfläche **Berechtigungen**) und Einstellungen für den Offline-Modus konfigurieren (Schaltfläche

Zwischenspeichern). Zusätzliche Informationen darüber finden Sie in der Windows-Hilfe.

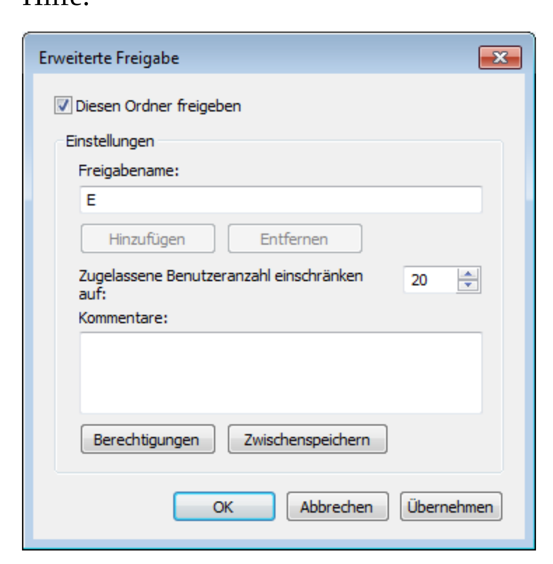


Abbildung 44: Erweiterte Freigabe

In Windows XP/Server 2003:

- Aktivieren Sie im Fenster **Eigenschaften von Lokaler Datenträger** in der Registerkarte **Freigabe** die Option **Diesen Ordner freigeben**. Geben Sie einen Namen für das freigegebene Objekt und die maximal zulässige Anzahl an Benutzern, die gleichzeitig darauf zugreifen können, an. Zusätzlich können Sie Zugriffsberechtigungen definieren (Schaltfläche **Berechtigungen**) und Einstellungen für den Offline-Modus konfigurieren (Schaltfläche **Zwischenspeichern**). Zusätzliche Informationen darüber finden Sie in der Windows-Hilfe.

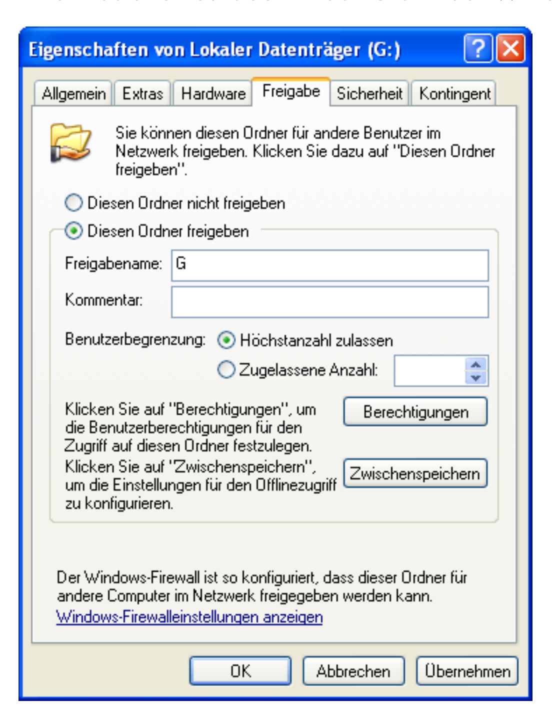


Abbildung 45: Freigabe des Ordners in Windows XP



Tipp. Wenn in der Registerkarte **Freigabe** die Option **Diesen Ordner freigeben** nicht abgebildet wird, dann öffnen Sie in der **Systemsteuerung** die **Ordneroptionen** und deaktivieren Sie in der Registerkarte **Ansicht** das Kontrollkästchen **Einfache Dateifreigabe verwenden (empfohlen)**.

5 Klicken Sie auf **Übernehmen**, dann auf **OK**.

Nun ist für Ihren Container der allgemeine Zugriff eingerichtet. Wenn der Container eingebunden ist, können andere Benutzer mit Ihren geschützten Daten arbeiten, indem sie den von Ihnen erstellten Netzwerkordner öffnen. Damit der Zugang zum Container stets gewährleistet werden kann, sollte der Computer, auf dem sich der von Ihnen angelegte Netzwerkordner befindet, zugänglich sein. Wenn auf einem Computer abwechselnd gearbeitet

werden soll, verwenden Sie die Funktion **Benutzer wechseln**, wenn Sie mit Ihrer Arbeit fertig sind. Diese Funktion erlaubt es, einen Benutzerwechsel ohne Abmeldung im System durchzuführen, wodurch eine stetige Bereitschaft des Netzwerkordners gewährleistet wird.

Um die gemeinsame Nutzung geschützter Daten wieder zu blockieren, deaktivieren Sie die Freigabe des Laufwerks (s. Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren auf S. 93).

Ebenso können Sie dazu den Container in ViPNet SafeDisk-V einfach trennen. Zum Aktivieren des allgemeinen Zugangs zum Container binden Sie diesen wieder ein (geben Sie bei der Einbindung das gleiche Laufwerk an, das zuvor freigegeben wurde).



Achtung! Nach einem Neustart des Computers muss der Netzwerkzugang zum Container neu eingestellt werden.

Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren

Zum Deaktivieren des Netzwerkzugangs auf den Container für andere Benutzer:

1. Deaktivieren Sie im Fenster **Erweiterte Freigabe** (s. Abbildung auf S. 91) das Kontrollkästchen **Diesen Ordner freigeben**.
2. Klicken Sie auf **Übernehmen** und dann auf **OK**.



Achtung! Nach einem Neustart des Computers sollte die Konfiguration des Netzwerkzugriffs auf den Container erneut durchgeführt werden.

Auf dem Server gespeicherte Daten schützen

Sie können ViPNet SafeDisk-V auf einem Server in Ihrem Netzwerk installieren. Dadurch können Sie zusätzlich:

- Unternehmensdaten, die auf dem Server gespeichert sind, schützen;
- den gleichzeitigen Zugriff mehrerer Benutzer auf sensible Daten auf dem Server gewährleisten;
- vermeiden, dass ViPNet SafeDisk-V auf mehreren Arbeitsstationen installiert werden muss, wodurch die Ausgaben für Software beträchtlich reduziert werden können.

Zum Schützen von Unternehmensdaten, die auf dem Server gespeichert sind:

1. Installieren Sie ViPNet SafeDisk-V auf dem Server.
2. Machen Sie sich mit dem Kapitel Vorgehensweise beim Datenschutz (auf S. 33) vertraut.
3. Erstellen Sie einen oder mehrere Container.
4. Binden Sie die erstellten Container ein und speichern Sie dort Daten ab, die für andere Benutzer zur Verfügung stehen sollen.
5. Aktivieren Sie mit Hilfe von Windows-Standardwerkzeugen die Freigabe für Laufwerke, die den neu erstellten Containern mit geschützten Daten zugeordnet sind (s. Netzwerkzugang auf einen Container für mehrere Benutzer ermöglichen auf S. 89). Anschließend können Ihre Mitarbeiter auf die Container wie auf normale Netzlaufwerke zugreifen.
6. Deaktivieren Sie die Freigabe der Laufwerke (s. Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren auf S. 93), um den allgemeinen Zugriff der Benutzer auf die sensiblen Daten wieder zu blockieren.

Der Einsatz von ViPNet SafeDisk-V auf einem Server unterscheidet sich kaum vom Einsatz des Programms auf einer einfachen Benutzer-Arbeitsstation. Mit Hilfe von ViPNet SafeDisk-V, das auf einem Server installiert ist, können Sie jederzeit folgende Aktionen durchführen:

- Eine Sicherungskopie der sensiblen Unternehmensdaten erstellen (s. Sicherungskopie der Containerschlüssel erstellen auf S. 39).
- Einen sicheren Datenaustausch zwischen den Computern sicherstellen. Unternehmensdaten sollten insbesondere bei Übertragungen über ein offenes Netzwerk oder bei Transporten mit Hilfe eines Kuriers (unter Verwendung eines mobilen Datenträgers oder eines Notebooks) zuverlässig geschützt werden. Wenn das Notebook oder der Datenträger verloren oder gestohlen wird, bleibt der Datenzugang weiterhin geschützt, da die Daten verschlüsselt sind.
- Den allgemeinen Zugriff auf Unternehmensdaten im „Gefahr“-Modus unverzüglich blockieren (s. Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus auf S. 99).
- Vertrauliche Unternehmensdaten im „Extreme Gefahr“-Modus unverzüglich vernichten (s. Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus auf S. 102).

Vertrauliche Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen

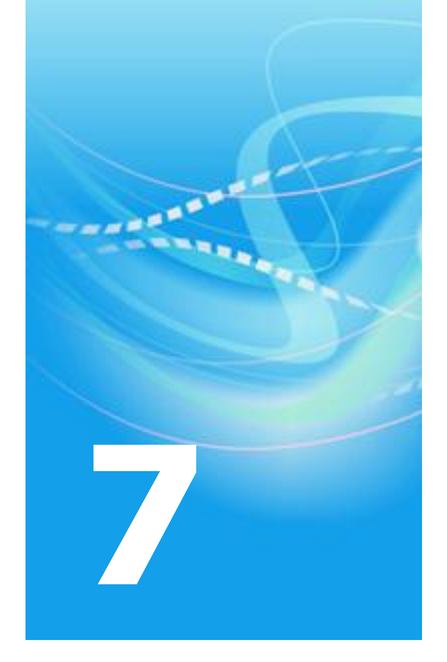
Beim Arbeiten mit Unternehmensdaten kann es manchmal erforderlich werden, sensible Informationen von einer Geschäftsstelle an eine andere zu übertragen. Wenn dabei das Notebook oder der Datenträger, die für den Transport verwendet werden, verloren gehen oder gestohlen werden, muss der Verlust von Daten unbedingt vermieden werden. Bei der Übertragung von Informationen über ungeschützte Netzwerkprotokolle (wie zum Beispiel FTP) können die Daten ebenfalls von Unbefugten abgefangen werden.

ViPNet SafeDisk-V ermöglicht es, Unternehmensdaten vor Verlusten während der Übertragung zu schützen.

Damit sensible Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen werden können:

1. Bereiten Sie die vertraulichen Daten für die Übertragung vor. Führen Sie dazu einen der folgenden Schritte aus:
   - Erstellen Sie eine Export-Datei des Containers (s. Container exportieren auf S. 65).
   - Erstellen Sie eine Sicherungskopie der Containerschlüssel (s. Sicherungskopie der Containerschlüssel erstellen auf S. 39) und kopieren diese zusammen mit der Container-Datei in einen Ordner.
2. Verschicken Sie die Daten über das Netzwerk oder übergeben diese an den Kurier.

Ausführliche Informationen dazu finden Sie im Kapitel Geschützte Daten exportieren und importieren (auf S. 62).



Arbeit in einer potentiell unsicheren Umgebung

Vorbereitung für den Einsatz in einer unsicheren Umgebung: Vorgehensweise

Damit Ihre vertraulichen Daten nicht in die Hände von Unbefugten geraten, sollten Sie alle Aufgaben aus der nachfolgenden Liste durchführen.

	Aufgabe	**Verweis**
☐	„Gefahr“ Modus aktivieren	Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus (auf S. 99)
☐	„Extreme Gefahr“ Modus aktivieren	Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus (auf S. 102)
☐	Hotkey-Tastenkombinationen für das schnelle Trennen und (oder) Vernichten aller Container merken	Tastenkombinationen (Hotkeys) für den „Gefahr“ und „Extreme Gefahr“ Modus (auf S. 105)



Tipp. Es wird empfohlen, die Liste auszudrucken und die einzelnen Punkte nach ihrer Abarbeitung zu markieren.

Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus

Wenn Sie der Meinung sind, dass die sich in Ihrer Umgebung befindlichen Außenstehenden eine Gefahr darstellen könnten, oder wenn Sie wissen, dass sich Unbefugte annähern, können Sie wie folgt vorgehen:

1 Führen Sie im Hauptfenster von ViPNet SafeDisk-V rechtzeitig eine der folgenden Aktionen aus:

   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Gefahr** .
   - Wählen Sie im Menü **Sicherheit** den Eintrag **„Gefahr“-Modus**.
   - Wählen Sie im Menü **SafeDisk** den Punkt **Einstellungen**, öffnen sie im Fenster **Einstellungen** die Registerkarte **„Gefahr“ Modus** und aktivieren Sie das Kontrollkästchen „Gefahr“ Modus. Klicken Sie anschließend auf **Übernehmen**.

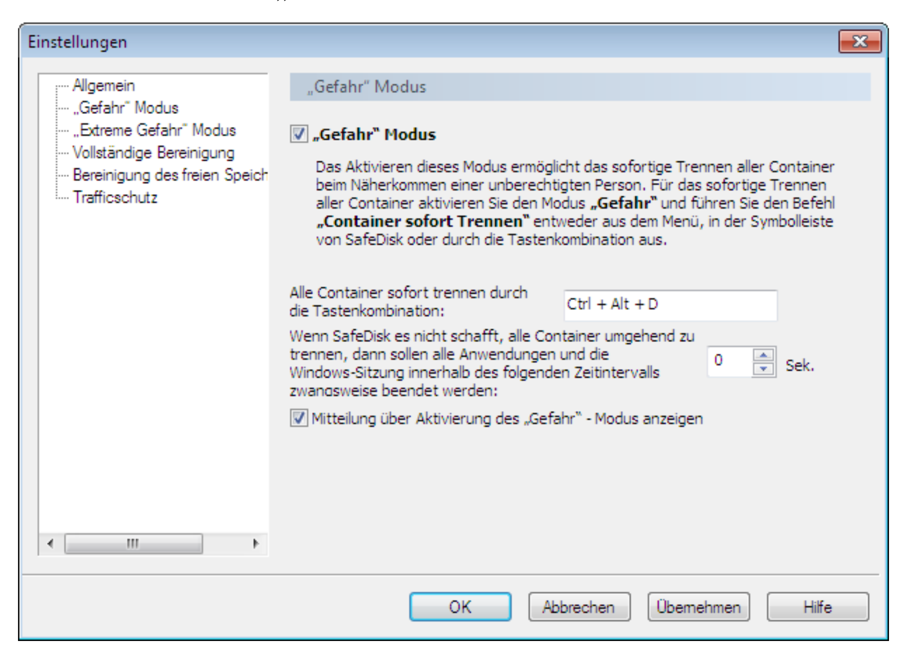


Abbildung 46: „Gefahr“ Modus aktivieren

„Gefahr“ Modus wird nun aktiviert.



Tipp. Wenn Sie nicht möchten, dass vom Programm Warnmeldungen über die Aktivierung des „Gefahr“- Modus eingeblendet werden, dann deaktivieren Sie entweder auf der Registerkarte **„Gefahr“ Modus** das Kontrollkästchen **Mitteilung über Aktivierung des „Gefahr“-Modus anzeigen** oder aktivieren Sie im Meldungsfenster „**Gefahr“-Modus aktivieren** das Kontrollkästchen **Dieses Fenster nicht mehr anzeigen**.

2 Wenn sich Unbefugte Ihrem Computer annähern, führen Sie eine der folgenden Aktionen aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Alle Container sofort trennen** .
- Wählen Sie im Menü **Sicherheit** den Befehl **Alle Container sofort trennen**.
- Drücken Sie die Tastenkombination **Strg**+**Alt**+**D** (standardmäßig eingestellte Kombination).



Tipp. Zum Ändern des Hotkey-Tastaturbefehls klicken Sie in der Registerkarte **„Gefahr“ Modus** (s. Abbildung auf S. 99) in das Eingabefeld **Alle Container sofort trennen durch die Tastenkombination** und drücken die Tastenkombination, die Sie einstellen wollen. Klicken Sie anschließend auf **Übernehmen**.

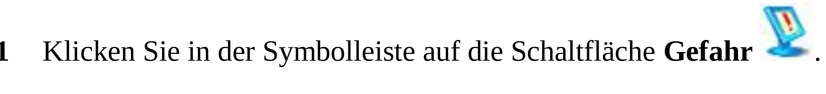
Alle Container werden sofort getrennt, der Zugang zu in diesen Containern gespeicherten Daten wird blockiert. Windows-Laufwerke, die den eingebundenen Containern zugeordnet sind, werden in der Ordnerübersicht Ihres Computers nicht mehr angezeigt. Das Programmfenster von ViPNet SafeDisk-V wird geschlossen, das Programmsymbol im Infobereich der Taskleiste wird ausgeblendet. Es bleiben keine Spuren übrig, die von Ihrer Arbeit mit vertraulichen Daten zeugen könnten.

Standardmäßig wird das sofortige Trennen der Container unverzüglich durchgeführt. Die Zeit der sofortigen Trennung der Container kann geändert werden, indem der benötigte Wert (in Sekunden) neben dem Feld **Wenn SafeDisk es nicht schafft, alle Container umgehend zu trennen, dann sollen alle Anwendungen und die Windows-Sitzung innerhalb des folgenden Zeitintervalls zwangsweise beendet werden** eingetragen wird. Es wird ausdrücklich davon abgeraten, diesen Parameter zu ändern. Wenn Sie diesen Parameter ändern und wenn ViPNet SafeDisk-V innerhalb der angegebenen Zeit (standardmäßig 0 Sekunden) nicht alle Container trennen kann, dann:

- werden alle eingebundenen Container zwangsweise getrennt,

- werden alle Anwendungen, die vom Benutzer gestartet wurden, geschlossen,
- wird die Arbeitssitzung des aktuellen Benutzers beendet.

Zum Deaktivieren des „Gefahr“ Modus:



1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Gefahr** .
2. Wählen Sie im Menü **Sicherheit** den Eintrag **„Gefahr“-Modu**s.
3. Deaktivieren Sie im Fenster **Einstellungen** in der Registerkarte **„Gefahr“ Modus** (s. Abbildung auf S. 99) das Kontrollkästchen **„Gefahr“ Modus** und klicken anschließend auf **Übernehmen**.

Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus

Der Modus „Extreme Gefahr“ ermöglicht es, alle in den Containern enthaltenen vertraulichen Daten schnell zu vernichten. Dies kann dann von Nutzen sein, wenn sich Ihnen Unbefugte annähern, und Sie keinen anderen Ausweg sehen, als alle sensiblen Informationen schnell zu löschen.



Achtung! Verwenden Sie den Modus „Extreme Gefahr“ nur in Ausnahmefällen. Container, die in diesem Modus gelöscht wurden, können nicht mehr wiederhergestellt werden.

Beim Löschen der Container im Modus „Extreme Gefahr“ werden die Containerschlüssel aller Benutzer vernichtet, und die in den Containern gespeicherten Daten gehen verloren.

Zum unverzüglichen Vernichten von vertraulichen Daten:

1 Führen Sie im Hauptfenster von ViPNet SafeDisk rechtzeitig eine der folgenden Aktionen aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Extreme Gefahr** .
- Wählen Sie im Menü Sicherheit den Punkt **„Extreme Gefahr“-Modus**.

- Wählen Sie im Menü **SafeDisk** den Punkt **Einstellungen**, öffnen im Fenster **Einstellungen** die Registerkarte **„Extreme Gefahr“ Modus** und aktivieren das Kontrollkästchen **„Extreme Gefahr“ Modus**. Klicken Sie anschließend auf **Übernehmen**.

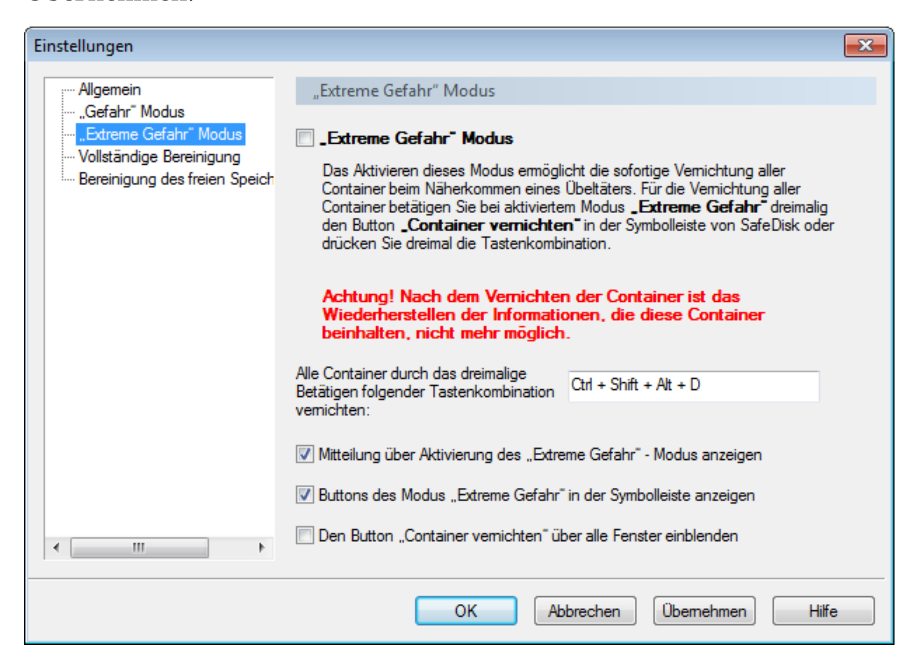


Abbildung 47: „Extreme Gefahr“-Modus aktivieren



Tipp. Wenn Sie nicht möchten, dass vom Programm Warnmeldungen über die Aktivierung des „Extreme Gefahr“- Modus eingeblendet werden, deaktivieren Sie entweder auf der Registerkarte **„Extreme Gefahr“ Modus** das Kontrollkästchen **Mitteilung über Aktivierung des „Extreme Gefahr“-Modus anzeigen** oder aktivieren Sie im Meldungsfenster **„Extreme Gefahr“-Modus aktivieren** das Kontrollkästchen **Dieses Fenster nicht mehr anzeigen**.

---

2 Zum sofortigen Vernichten vertraulicher Daten klicken Sie in der Symbolleiste dreimal auf die Schaltfläche **Alle Container vernichten** oder drücken dreimal in Folge die Hotkey-Tastenkombination **Strg+Umschalt+Alt+D**.



Tipp. Zum Ändern des Hotkey-Tastaturbefehls klicken Sie in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf S. 103) in das Eingabefeld **Alle Container durch das dreimalige Betätigen folgender Tastenkombination vernichten** und drücken die Tastenkombination, die Sie einstellen wollen. Klicken Sie anschließend auf **Übernehmen**.

Alle Container, Containerschlüssel und Sicherungskopien der Konfiguration werden sofort vernichtet. Das Programmfenster von ViPNet SafeDisk-V wird geschlossen, das Symbol im Infobereich der Taskleiste wird ausgeblendet. Wenn ViPNet SafeDisk-V es nicht schafft, innerhalb der angegebenen Zeit (standardmäßig 60 Sekunden) alle Container zu trennen, dann:

- werden alle eingebundenen Container zwangsweise getrennt,
- werden alle Anwendungen, die vom Benutzer gestartet wurden, geschlossen,
- wird die Arbeitssitzung des aktuellen Benutzers beendet.

Beim nächsten Programmstart wird die Container-Liste leer.

Sie können die Schaltflächen des „Extreme Gefahr“ Modus von der ViPNet SafeDisk Symbolleiste entfernen. Dazu:

1 Deaktivieren Sie im Fenster **Einstellungen** in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf S. 103) das Kontrollkästchen **Buttons des Modus „Extreme Gefahr“ in der Symbolleiste anzeigen**.

2 Klicken Sie auf **Übernehmen**.

Sie können zusätzlich die halbtransparente Schaltfläche **Alle Container vernichten** im rechten unteren Bereich Ihres Desktops aktivieren. Führen Sie dafür die folgenden Schritte durch:

1 Aktivieren Sie Im Fenster **Einstellungen** in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf S. 103) das Kontrollkästchen **Den Button „Container vernichten“ über alle Fenster einblenden**.

2 Klicken Sie auf **Übernehmen**.

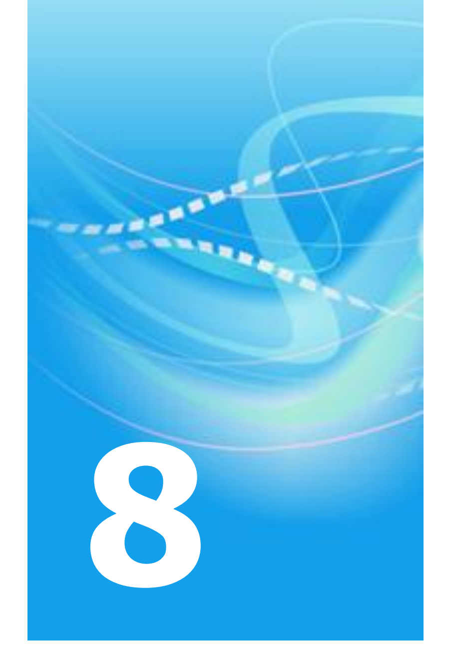
Zum Deaktivieren des „Extreme Gefahr“ Modus führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Extreme Gefahr** .
- Wählen Sie im Menü **Sicherheit** den Eintrag **„Extreme Gefahr“-Modus**.
- Deaktivieren Sie im Fenster **Einstellungen** in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf S. 103) das Kontrollkästchen **„Extreme Gefahr“ Modus** und klicken anschließend auf **Übernehmen**.

Tastenkombinationen (Hotkeys) für den „Gefahr“ und „Extreme Gefahr“ Modus

Strg+Alt+D – drücken Sie diese Tastenkombination, um unverzüglich alle Container zu trennen (Modus „Gefahr“ muss dabei aktiviert sein).

Strg+Umschalt+Alt+D – drücken Sie diese Tastenkombination dreimal in Folge, um unverzüglich alle Ihre Container zu vernichten (Modus „Extreme Gefahr“ muss dabei aktiviert sein).



Spurenbeseitigung bei der Arbeit mit privaten Daten

Warum Datenspuren bereinigt werden müssen

Das Betriebssystem Windows ermöglicht es, Dateien wiederherzustellen, falls Sie diese aus Versehen gelöscht, den Papierkorb bereinigt oder die Dateien mit Hilfe der Tastenkombination **Umschalt+Entf** entfernt haben. Die Wiederherstellung der Daten ist auch dann möglich, wenn das Laufwerk formatiert wurde oder wenn die Festplatte ausgefallen ist und alle Daten als verloren gemeldet wurden.

Wenn Sie eine Datei durch Anwendung von Standardmethoden löschen, bleiben die Daten physikalisch auf der Festplatte erhalten. Das Betriebssystem vermerkt lediglich die Datei als gelöscht, indem es den Dateinamen ändert. Später können an der Stelle der Datei andere Daten gespeichert werden.

Nach der Formatierung der Festplatte bleibt eine zuvor erstellte Sicherungskopie übrig. Wenn es zum Ausfall der Festplatte kommt, können die Daten mit Hilfe physikalischer Methoden wiederhergestellt werden.

Das bedeutet, dass Sie Ihre privaten Daten ohne Anwendung zusätzlicher Werkzeuge nicht sicher und zuverlässig löschen können. Im Lieferumfang von ViPNet SafeDisk-V ist die Utility Clean.exe enthalten, die für das vollständige Löschen von ungeschützten Daten sorgt.



Hinweis. Daten, die mit Hilfe von ViPNet SafeDisk-V geschützt sind, werden immer zuverlässig bereinigt

Das sichere Löschen von Daten kann in folgenden Situationen erforderlich sein:

- Sie haben im Programm MS Word an einem sensiblen Dokument gearbeitet. Auch wenn Sie das Dokument in einem ViPNet SafeDisk-V-Container aufbewahren, bleiben im Betriebssystem Windows Informationen darüber, welche Datei wann, von wem und an welchem Speicherort geöffnet wurde. Aus Sicherheitsgründen sollten Sie diese Informationsspuren bereinigen.
- Sie haben eine Transaktion im Internet durchgeführt, bei welcher Sie Ihre persönlichen und finanziellen Daten verwendet haben. Die Spuren dieses Vorgangs bleiben in Cookie-Dateien und in temporären Internet-Dateien erhalten. Diese Daten sollten aus Selbstschutzgründen vollständig gelöscht werden.

- Sie haben einen neuen Computer gekauft und wollen den alten Rechner verkaufen. Sie haben die Festplatte des Rechners mit Hilfe herkömmlicher Werkzeuge von Windows formatiert, um mögliche Spuren vertraulicher Daten, mit denen Sie auf dem alten Computer gearbeitet haben, zu entfernen. Es gibt jedoch Verfahren, die es ermöglichen, die Daten auf einer formatierten Festplatte wiederherzustellen. Um sicherzustellen, dass Ihre privaten Daten nicht nachträglich weiterverwendet werden, sollten Sie mit Hilfe der Funktionalität von ViPNet SafeDisk-V den freien Speicherplatz auf den Laufwerken regelmäßig bereinigen.

Vorgehensweise beim Bereinigen von Datenspuren

Wenn Sie mit unterschiedlichen Dateien gearbeitet, Texte kopiert, Dateien aus einem Ordner in einen anderen verschoben oder Dateien mit Hilfe von Standardwerkzeugen gelöscht haben, sollten Sie regelmäßig dafür sorgen, die verbliebenen Datenfragmente sicher und vollständig zu bereinigen.

Mit Hilfe der Bereinigungsfunktionalität von ViPNet SafeDisk können Sie Ihre Arbeitsspuren zuverlässig löschen. Zuerst müssen Sie die zu bereinigenden Objekte bestimmen. Sie können Ihre Arbeitsspuren im Betriebssystem Windows und im Internet Explorer bereinigen.

Mit Hilfe von ViPNet SafeDisk-V können im Betriebssystem Windows folgende Objekte bereinigt werden:

- Zuletzt verwendete Dokumente.
- Temporäre Dateien.
- Papierkorb.
- Freier Speicherplatz auf den Laufwerken, auf denen Daten vor ihrer Übertragung in ViPNet SafeDisk-V-Container gespeichert waren.

Weitere Details zur Handhabung der aufgezählten Objekte finden Sie im Kapitel Datenspuren in Windows bereinigen (auf S. 112).

Ebenso können folgende Internet Explorer Objekte bereinigt werden:

- Verlauf.
- Temporäre Internetdateien.
- Cookie-Dateien.

Weitere Details zur Handhabung der aufgezählten Objekte finden Sie im Kapitel Datenspuren im Internet Explorer bereinigen (auf S. 117).

ViPNet SafeDisk-V ermöglicht es, mit Hilfe der Funktion **Vollständige Bereinigung (auf S. 120)** ein vollständiges Entfernen aller Spuren vertraulicher Daten zeitgleich durchzuführen**.**

Wenn Sie ein erfahrener Benutzer oder Programmierer sind, können Sie die Utility Clean.exe (s. Bereinigung über die Befehlszeile starten auf S. 123) verwenden, um die vollständige Bereinigung von Datenspuren mit Hilfe eines Kommandozeilenbefehls durchzuführen.

Bereinigung von Datenspuren: Reihenfolge der Schritte

Wenn Sie sicher sein wollen, dass Sie die Datenspuren sicher bereinigt haben, führen Sie alle Schritte aus der nachfolgenden Tabelle durch.

	Aufgabe	Verweis
☐	Liste der zuletzt verwendeten Dokumente regelmäßig löschen	Liste zuletzt verwendeter Dateien löschen (auf S. 112)
☐	Temporäre Dateien regelmäßig löschen	Temporäre Dateien löschen (auf S. 112)
☐	Papierkorb regelmäßig bereinigen	Papierkorb bereinigen (auf S. 113)
☐	Spuren verschobener oder gelöschter ungeschützter Dateien regelmäßig bereinigen	Sicheres Löschen ungeschützter Dateien (auf S. 113)
☐	Freien Speicherplatz auf der Festplatte regelmäßig bereinigen	Freien Speicherplatz auf Laufwerken bereinigen (auf S. 114)
☐	Browserverlauf regelmäßig löschen	Datenspuren im Internet Explorer bereinigen (auf S. 117)
☐	Temporäre Internetdateien regelmäßig entfernen	Temporäre Internetdateien löschen (auf S. 117)
☐	Cookie-Dateien regelmäßig bereinigen	Cookies bereinigen (auf S. 118)



Tipp. Es wird empfohlen, die Liste auszudrucken und die einzelnen Punkte nach ihrer Abarbeitung zu markieren.

Datenspuren in Windows bereinigen

Liste zuletzt verwendeter Dateien löschen

Windows ermöglicht eine schnellere Suche nach vor Kurzem geöffneten Dokumenten, indem Verweise auf diese Dokumente im Ordner **Zuletzt verwendete Dokumente** gespeichert werden. Dieser Ordner kann über das Menü **Start** aufgerufen werden. Anhand dieser Verweise können Unbefugte Informationen über die Existenz sensibler Daten erhalten. Aus Sicherheitsgründen sollte der Ordner **Zuletzt verwendete Dokumente** regelmäßig geleert werden.

ViPNet SafeDisk-V entfernt auf eine sichere Art und Weise Links auf kürzlich geöffnete Dokumente aus den nachfolgenden Ordnern:

- `C:\Users\Benutzername\AppData\Roaming\Microsoft\Windows\Recent` (in Vista und späteren Versionen von Windows).
- `C:\Users\Benutzername\AppData\Roaming\Microsoft\Office\Recent` (in Vista und späteren Versionen von Windows).
- `C:\Documents and Settings\Benutzername\Recent` (in Windows XP).

Zum Bereinigen des Ordners **Zuletzt verwendete Dokumente**:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken anschließend auf **Windows Arbeitsverlauf**.
2. Dadurch werden alle Verweise auf kürzlich geöffnete Dokumente gelöscht.



Tipp. Sie können ViPNet SafeDisk-V so einstellen, dass die Liste der zuletzt verwendeten Dokumente automatisch beim Beenden jeder Arbeitssitzung bereinigt wird (s. Parameter von ViPNet SafeDisk-V einstellen auf S. 58).

Temporäre Dateien löschen

Viele Windows-Anwendungen erstellen beim Öffnen von Dokumenten temporäre Dateien. Diese Dateien können eine vollständige Kopie der Originaldatei sowie weitere System- und Zusatzinformationen enthalten. In der Regel werden temporäre Dateien automatisch gelöscht,

wenn die Originaldatei geschlossen wird. In einigen Fällen werden neu angelegte temporäre Dateien jedoch nicht entfernt. Diese „vergessenen“ temporären Dateien, die vertrauliche Daten enthalten, können eine ernsthafte Gefahr für die Informationssicherheit des Unternehmens darstellen. Deswegen müssen bei Handhabung sensibler Daten die von unterschiedlichen Anwendungen zurückgelassenen temporären Dateien regelmäßig auf eine sichere Art und Weise gelöscht werden.

ViPNet SafeDisk-V entfernt auf sichere Art und Weise temporäre Dateien aus den nachfolgenden Ordnern:

- `C:\WINDOWS\Temp` (oder ein anderer Ordner, der im System als Standardordner für temporäre Dateien definiert ist).
- `C:\Documents and Settings\Benutzername\Local Settings\Temp` (in Windows XP:).
- `C:\Users\Benutzername\AppData\Local\Temp` (in Vista und späteren Versionen von Windows).

Zum Löschen von temporären Dateien:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken anschließend auf **Temporäre Dateien**.
2. Dadurch werden alle temporären Dateien, die von unterschiedlichen Anwendungen angelegt wurden, sicher gelöscht.

Papierkorb bereinigen

Dateien, die mit herkömmlichen Mitteln gelöscht wurden, werden in den **Papierkorb** verschoben und können leicht wiederhergestellt werden. Damit ein Wiederherstellen gelöschter Dateien aus dem **Papierkorb** verhindert wird, müssen Sie den **Papierkorb** zuverlässig bereinigen.

Zum Bereinigen des **Papierkorbs**:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken anschließend auf **Papierkorb**.
2. Dadurch wird der gesamte Inhalt von **Papierkorb** sicher gelöscht.

Sicheres Löschen ungeschützter Dateien

Bevor Sie ViPNet SafeDisk-V auf Ihrem Computer installiert haben, wurden vertrauliche Daten ungeschützt auf der Festplatte gespeichert. Wie Sie wissen, kann diese Art der Speicherung

nicht den benötigten Umfang an Informationssicherheit gewährleisten. Sogar nach dem Löschen der Dateien von der Festplatte und dem anschließenden Leeren des Papierkorbs können Daten mit Hilfe spezieller Werkzeuge oder physikalischer Eingriffe wiederhergestellt werden.

Nach der Installation von ViPNet SafeDisk-V haben Sie alle Dateien, die sensible Informationen beinhalten, in geschützte Container verschoben. Diese Dateien können aber immer noch auf der Festplatte leicht wiederhergestellt werden. Um diese Gefahrenquelle zu beseitigen, sollten die Dateien nach dem Verschieben vollständig und sicher von der Festplatte entfernt werden.

Zum sicheren Löschen von ungeschützten Dateien führen Sie einen der folgenden Schritte aus:

- Löschen Sie die Dateien auf eine sichere Art und Weise (s. Dateien sicher löschen auf S. 114).
- Wenn Sie die Dateien mit Hilfe herkömmlicher Mittel von Windows bereits gelöscht haben, verwenden Sie ViPNet SafeDisk-V dazu, freien Speicherplatz auf der Festplatte zu bereinigen (s. Freien Speicherplatz auf Laufwerken bereinigen auf S. 114).

Dateien sicher löschen

Zum sicheren Löschen von Dateien:

1. Markieren Sie die betroffene Datei im ungeschützten Ordner.
2. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie im Kontextmenü den Eintrag **Sicheres Löschen** (in Windows 7 und in früheren Windows-Versionen als Vista können Sie auch in der Ordnerübersicht im Menü **Datei** den Befehl **Sicheres Löschen** auswählen).
3. Klicken Sie im Fenster **Sicheres Löschen** bestätigen auf **Ja**.

Freien Speicherplatz auf Laufwerken bereinigen

Zum Bereinigen des freien Festplattenspeichers:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken Sie anschließend auf **Freier Speicherplatz**. Es wird der Assistent **Sicheres Löschen** gestartet.
2. Aktivieren Sie auf der Seite **Freier Speicherplatz auf den Laufwerken** die Kontrollkästchen neben den Laufwerken, die Sie bereinigen möchten, und klicken Sie auf **Weiter**.

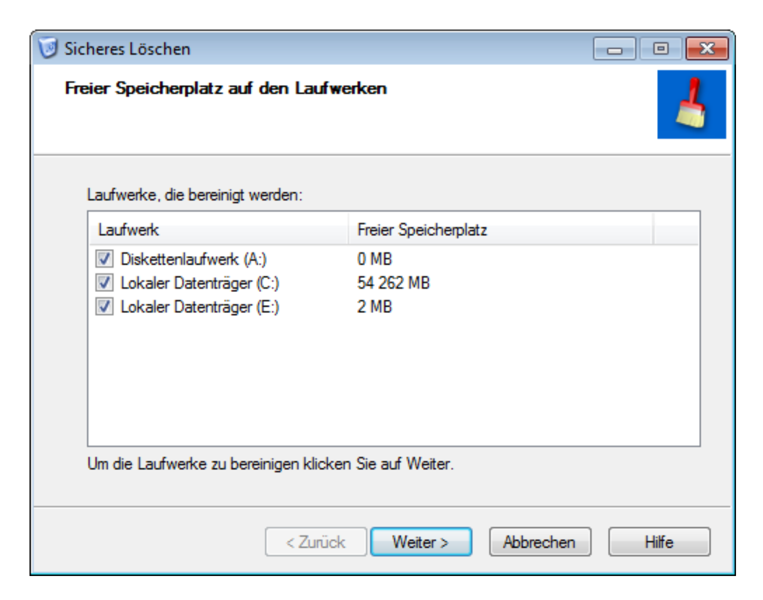


Abbildung 48: Freien Speicherplatz auf den Laufwerken bereinigen

3 Warten Sie, bis der Bereinigungsvorgang abgeschlossen ist.

4 Klicken Sie auf der Seite **Bereinigung wird abgeschlossen** auf die Schaltfläche **Fertig**.

Laufwerke für standardmäßige Bereinigung des freien Speicherplatzes einstellen

Zum Einstellen von Laufwerken für eine automatische Bereinigung des freien Speicherplatzes:

1 Wählen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **SafeDisk** den Eintrag **Einstellungen**.

2 Öffnen Sie im Fenster **Einstellungen** die Registerkarte **Bereinigung des freien Speicherplatzes**.

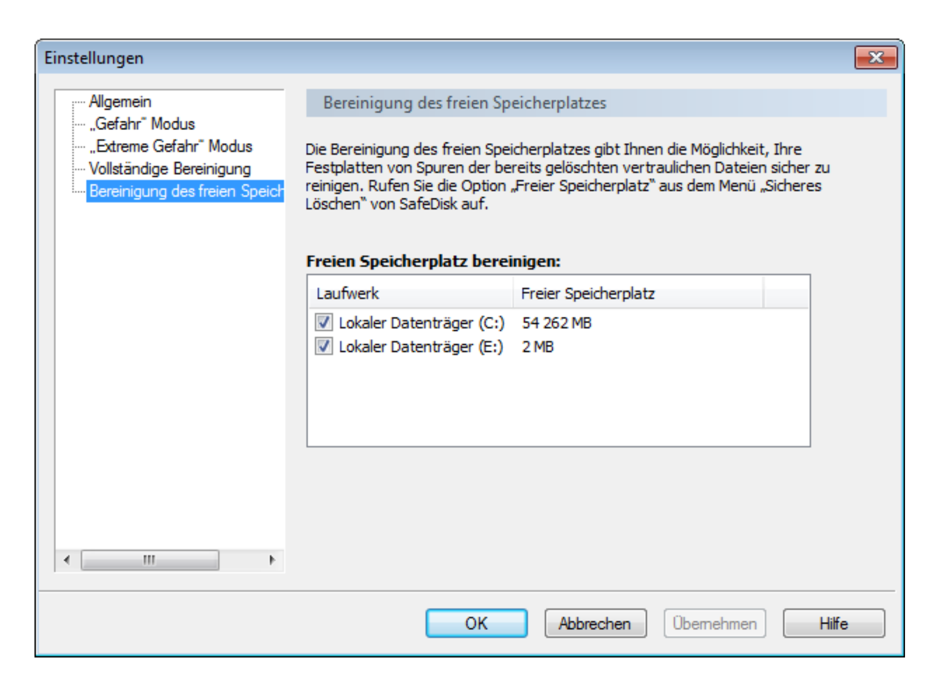


Abbildung 49: Laufwerke für Speicherbereinigung auswählen

3 Aktivieren Sie in der Liste **Freien Speicherplatz bereinigen** die Kontrollkästchen neben den Laufwerken, die Sie standardmäßig bereinigen möchten.

4 Klicken Sie auf **Übernehmen** und dann auf **OK**.

Datenspuren im Internet Explorer bereinigen



Achtung! Die Bereinigung des Browserverlaufs, der temporären Internetdateien und Cookies wird nur für den Browser MS Internet Explorer durchgeführt. Die Bereinigung der Browser anderer Hersteller wird in nachfolgenden Versionen von ViPNet SafeDisk-V implementiert.

Browserverlauf leeren

Wenn Sie sich Webseiten anzeigen lassen, speichert Internet Explorer Informationen über die von Ihnen besuchten Seiten ab (standardmäßig wird der Browserverlauf der letzten 3 Wochen gespeichert). Die Liste der besuchten Webseiten hilft dabei, schneller zu den früher aufgerufenen Seiten zurückzukehren. Wenn Sie aber nicht wollen, dass diese Informationen für Andere zugänglich sind, sollten Sie den Browserverlauf regelmäßig löschen.

Der Internet Explorer Browserverlauf wird in folgenden Ordnern gespeichert:

- `C:\Documents and Settings\Benutzername\Local Settings\History` (in Windows XP);
- `C:\Users\Benutzername\AppData\Local\Microsoft\Windows\History` (in Vista und späteren Versionen von Windows)

Zum Bereinigen des Browserverlaufs vom Internet Explorer:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **Sicheres Löschen** auf den Eintrag **Internet Explorer** und klicken anschließend auf **Verlauf**.
2. Dadurch werden alle Informationen über die von Ihnen besuchten Webseiten gelöscht.

Temporäre Internetdateien löschen

Beim Arbeiten mit Webseiten speichert Internet Explorer alle Daten ab, die er aus dem Internet erhält. Das kann dann von Nutzen sein, wenn für den Internetzugang eine langsame Modem-Verbindung verwendet wird, da so die Ladegeschwindigkeit von Web-Inhalten gesteigert

werden kann. Wenn Sie aber nicht wollen, dass diese Daten für Andere zugänglich werden, sollten Sie die temporären Internetdateien regelmäßig löschen.

Internet Explorer speichert die temporäre Dateien in folgenden Ordnern ab:

- `C:\Documents and Settings\Benutzername\Local Settings\Temporary Internet Files` (in Windows XP).
- `C:\Users\Benutzername\AppData\Local\Microsoft\Windows\Temporary Internet Files` (in Vista und späteren Versionen von Windows).

Zum Löschen temporärer Internetdateien:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Internet Explorer** und klicken anschließend auf **Temporäre Dateien**.
2. Dadurch werden alle temporären Internetdateien auf sichere Art und Weise gelöscht.

Cookies bereinigen

Eine Cookie-Datei stelle eine Textdatei dar, die vom Internet-Browser auf dem Computer abgespeichert wird. In diesen Dateien können Inhalte von Warenkörben eines Online-Shops, Namen und Passwörter von Benutzerkonten unterschiedlicher Webseiten sowie andere private Daten abgelegt werden. Um diese Daten unzugänglich zu machen, müssen die Cookie-Dateien gelöscht werden.



Achtung! Damit Cookie-Dateien erfolgreich gelöscht werden können, muss Internet Explorer zuvor beendet werden.

Internet Explorer speichert die Cookie-Dateien in den folgenden Ordnern ab:

- In Windows XP:
  - `C:\Documents and Settings\Benutzername\Cookies.`
  - `C:\Documents and Settings\Benutzername\Local Settings\Temporary Internet Files.`
- In Windows Vista und späteren Windows-Versionen:
  - `C:\Users\Benutzername\AppData\Roaming\Microsoft\Windows\Cookies.`
  - `C:\Users\Benutzername\AppData\Local\Microsoft\Windows\Temporary Internet Files.`

Zum Löschen von Cookie-Dateien:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **Sicheres Löschen** auf den Eintrag **Internet Explorer** und klicken anschließend auf **Cookies**.
2. Dadurch werden alle Cookie-Dateien, die vertrauliche Daten enthalten könnten, auf sichere Art und Weise gelöscht.

Vollständige Bereinigung

Wenn nötig, können Sie gleichzeitig mehrere Typen von Objekten bereinigen, um alle Spuren der Arbeit mit vertraulichen Daten zu vernichten. Dazu:

1. Wählen Sie im Hauptfenster von ViPNet SafeDisk-V im Menü **Sicheres Löschen** den Eintrag **Vollständige Bereinigung**. Es wird der Assistent **Vollständige Bereinigung** gestartet.

2. Aktivieren Sie auf der Seite **Vollständige Bereinigung** in der Liste **Bereinigen** die Kontrollkästchen neben den Objekten, die Sie bereinigen möchten.

   Klicken Sie auf **Weiter**.

   Abbildung 50: Assistent für die vollständige Bereinigung

3. Aktivieren Sie auf der Seite **Freier Speicherplatz** auf den Laufwerken das Kontrollkästchen **Freien Speicherplatz auf Laufwerken bereinigen**, wenn Sie den freien Speicherplatz auf der Festplatte von Spuren gelöschter oder verschobener sensibler Dokumente bereinigen möchten.

   Aktivieren Sie in der Liste **Laufwerke, die bereinigt werden** die Kontrollkästchen neben den Laufwerken, die Sie bereinigen möchten. Klicken Sie anschließend auf **Weiter**.

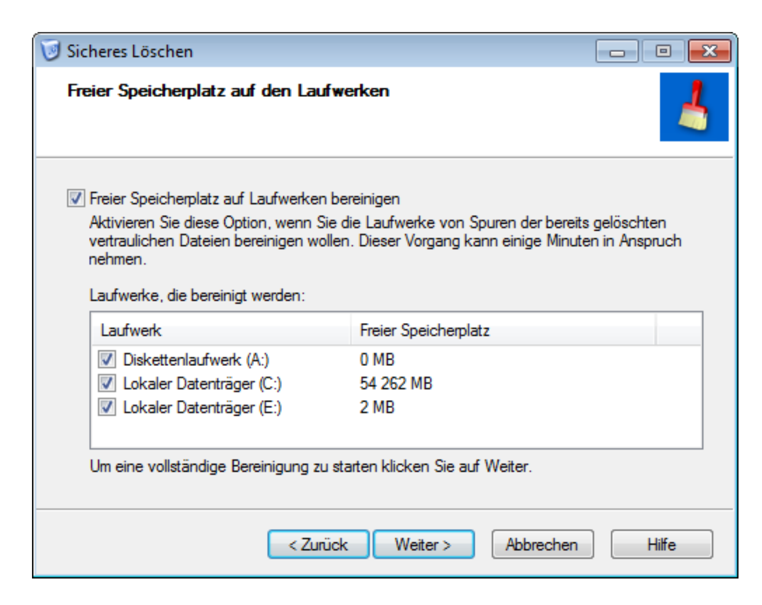


Abbildung 51: Laufwerke für Bereinigung des freien Speicherplatzes auswählen

4 Auf der Seite **Bereinigung wird beendet** wird angezeigt, welche Arten von Arbeitsspuren bei Verwendung vertraulicher Daten bereinigt wurden.



Abbildung 52: Bereinigung abschließen

Zum Abschluss des Assistenten klicken Sie auf die Schaltfläche **Fertig**.

Vollständige Bereinigung einstellen

Damit Sie festlegen können, welche Daten beim Durchführen einer vollständigen Bereinigung sicher gelöscht werden sollen, gehen Sie wie folgt vor:

1. Wählen Sie im Menü **SafeDisk** den Punkt **Einstellungen**.
2. Öffnen Sie im Fenster **Einstellungen** die Registerkarte **Vollständige Bereinigung**.

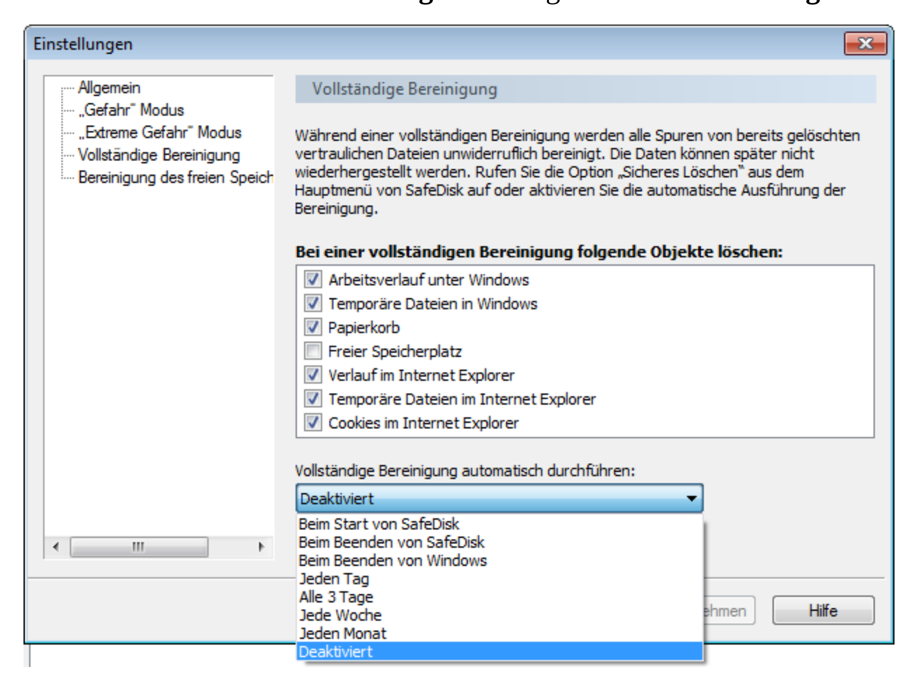


Abbildung 53: Bereiche für die vollständige Bereinigung definieren

3. Aktivieren Sie auf der Registerkarte **Vollständige Bereinigung** in der Liste **Bei einer vollständigen Bereinigung folgende Objekte löschen** die Kontrollkästchen neben den Objekten, die Sie standardmäßig bereinigen wollen.
4. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Damit die vollständige Bereinigung automatisch durchgeführt wird:

1. Wählen Sie im Fenster **Einstellungen** auf der Registerkarte Vollständige Bereinigung (s. Abbildung auf S. 120) in der Dropdownliste **Vollständige Bereinigung automatisch durchführen** einen der folgenden Einträge aus: **Beim Start von SafeDisk**, **Beim Beenden von SafeDisk**, **Beim Beenden von Windows**, **Jeden Tag**, **Alle 3 Tage**, **Jede Woche**, **Jeden Monat**, **Deaktiviert**.
2. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Bereinigung über die Befehlszeile starten

ViPNet SafeDisk-V ermöglicht die Benutzung der Befehlszeile, um unterschiedliche Bereinigungsvorgänge zu starten. Dies kann in folgenden Fällen von Nutzen sein:

- Es müssen Spuren von Dateien eines bestimmten Typs bereinigt werden. Sie möchten zum Beispiel die Spuren aller `*.doc`-Dateien vernichten, da gerade die Dateien dieses Typs sensible Daten beinhalten.
- Es muss ein bestimmter Ordner auf der Festplatte bereinigt werden.
- Sie haben eine Batch-Datei (`*.bat`) erstellt und wollen darin die Bereinigungsbefehle von ViPNet SafeDisk-V verwenden. Zum Beispiel wollen Sie die Bereinigung mit Hilfe von ViPNet SafeDisk-V gemäß einem Zeitplan ohne weitere Benutzer-Interaktionen durchführen oder jedes Mal vor dem Ausschalten des Computers starten lassen.
- Sie haben ein Plug-In für Microsoft Word erstellt, um mit bestimmten Daten sicher arbeiten zu können. Die Sicherheitsanforderungen an dieses Plug-In erfordern die Vernichtung aller Arbeitsspuren nach der Handhabung vertraulicher Dokumente in Microsoft Word.
- Es müssen Bereinigungsbefehle von ViPNet SafeDisk-V ausgeführt werden, ohne dabei die graphische Benutzeroberfläche von ViPNet SafeDisk-V zu starten. Zum Beispiel wollen Sie es zu diesem Zeitpunkt vermeiden, andere Benutzer von ihren Aufgaben abzulenken.

Gehen Sie wie folgt vor, um Bereinigungsbefehle von ViPNet SafeDisk-V über eine Befehlszeile zu starten:

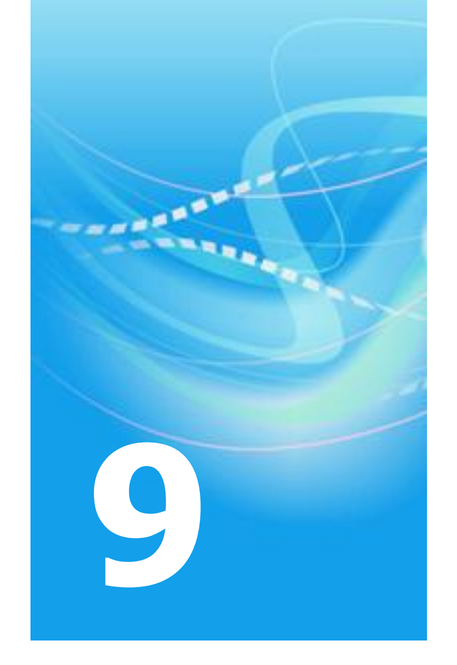
1. Starten Sie den Befehlszeileninterpreter.
2. Geben Sie den Pfad zur Utility-Datei `Clean.exe` ein. Standardmäßig befindet sich die Utility im Ordner `C:\Program Files\InfoTeCS\ViPNet SafeDisk\`.
3. Tippen Sie in der Befehlszeile die folgende Zeichenfolge ein: clean.exe – Leerzeichen – Schrägstrich (/) – benötigter Parameter. Die möglichen Parameter sind mitsamt der Beschreibung in der nachfolgenden Tabelle aufgelistet.

Tabelle 5. Befehle der Bereinigung in ViPNet SafeDisk-V

Befehle im Menü ViPNet SafeDisk-V (graphische Benutzeroberfläche)	**Befehle in der Befehlszeile (mit Parametern)**	**Ergebnisse**
Windows		
Freier Speicherplatz	`Clean.exe /f <Laufwerksbuchstabe>`	Der freie Speicherplatz auf dem ausgewählten Laufwerk wird bereinigt. Um freien Speicherplatz auf einem Laufwerk bereinigen zu können, müssen Sie über Schreibrechte für den Stammordner des Laufwerks verfügen.
Temporäre Dateien	`Clean.exe /t`	Temporäre Windows-Dateien werden sicher gelöscht.
Arbeitsverlauf	`Clean.exe /d`	Alle Verweise im Ordner **Zuletzt verwendete Dokumente** werden sicher gelöscht.
Papierkorb	`Clean.exe /r`	Papierkorb wird sicher bereinigt.
	`Clean.exe <Dateimaske>`	Dateien, die zur definierten Maske passen, werden aus dem angegebenen Ordner (standardmäßig aus dem aktuellen Ordner) entfernt. Beim Definieren der Maske gilt Folgendes: ? – ersetzt genau ein Symbol. * – ersetzt mehrere Symbole. Wenn Sie zum Beispiel die Maske *.doc definieren, werden alle Dateien mit der Erweiterung .doc entfernt.
	`Clean.exe <Ordnernahme>`	Ordnerinhalt wird gelöscht.
Internet Explorer		
Verlauf	Clean.exe /h	Browserverlauf im Internet Explorer wird bereinigt.
Temporäre Dateien	`Clean.exe /i`	Temporäre Internetdateien werden gelöscht.
Cookies	`Clean.exe /c`	Cookies werden gelöscht.



Tipp. Sie können die Utility Clean.exe mit mehreren Parametern gleichzeitig starten. Zum Beispiel: `Clean.exe /c /h /i /t /r /d /fc c:\folder1\*.* c:\folder2`.



Suche und Beseitigung von Störungen

Logdatei anzeigen

Zum Anzeigen der Logdatei von ViPNet SafeDisk-V:

1. Öffnen Sie den Programmordner. Standardmäßig wird ViPNet SafeDisk-V in den folgenden Ordner installiert: `C:\Users\All Users\InfoTeCS\safedisk-v`.
2. Öffnen Sie die Datei `SDEvents.log`. Die Datei enthält Informationen über folgende Ereignisse:
   - Benutzeranmeldung im Programm.
   - Benutzerabmeldung im Programm.
   - Aktivierung des „Gefahr“ Modus.
   - Aktivierung des „Extreme Gefahr“-Modus.
   - Alle Vorgänge, die sich auf Container beziehen (unter Angabe des Containernamens): Erstellung eines neuen Containers, Einbindung des Containers, Trennen des Containers, Löschen des Containers, Container-Import, Container-Export, Änderung der Container-Eigenschaften.

Für jedes Ereignis werden folgende Daten registriert:

- Ereignisdatum und –zeit.
- Ereignisstatus: erfolgreicher Abschluss oder Abbruch.

Typische Problemfälle

ViPNet Safe Disk-V kann nicht gestartet werden

Beim Starten von ViPNet Safe Disk-V kann das Programm folgende Fehlermeldungen ausgeben:

- Programm kann nicht gestartet werden. ViPNet ist nicht installiert.
- Programm kann nicht gestartet werden. Ordner der ViPNet Schlüsseldistribution nicht gefunden.
- Programm kann nicht gestartet werden. Diesem Netzwerkknoten wurde die Rolle „Safe Disk" nicht zugeordnet.
- Programm kann nicht gestartet werden. Die Gültigkeitsdauer der Lizenz ist abgelaufen.

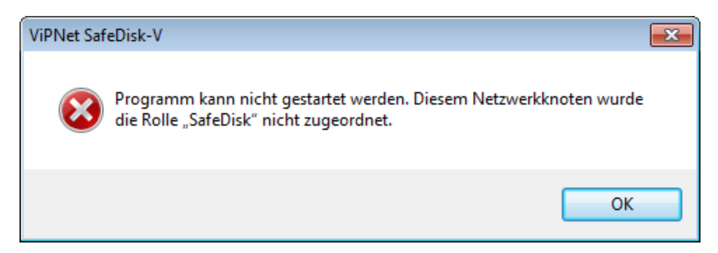


Abbildung 54: Fehler beim Starten von ViPNet Safe Disk-V

Diese Fehler können auftreten, wenn eine oder mehrere Bedingungen für die Integration von ViPNet Safe Disk-V mit ViPNet Client nicht erfüllt sind (s. Anforderungen an die Softwareumgebung auf S. 11).

Container ist nicht verfügbar

Wenn beim Versuch, einen neuen Container einzubinden, die Meldung eingeblendet wird, dass der Container nicht verfügbar ist:

1. Öffnen Sie den Ordner **Arbeitsplatz**.
2. Drücken Sie die Taste **F5**, um den Ordner zu aktualisieren. Ein neues lokales Laufwerk wird angezeigt.

Formatieren Sie den Container, bevor Sie ihn verwenden.

Laufwerk kann nicht formatiert werden

Wenn das Programm ViPNet SafeDisk-V auf einem Computer mit dem Betriebssystem Windows installiert ist, und Sie über keine Administratorrechte in diesem System verfügen, dann können Sie das Laufwerk des Containers nicht formatieren. Um dieses Problem zu lösen, müssen Sie entweder Administratorrechte erlangen oder Ihren Systemadministrator bitten, den Container für Sie zu erstellen und auf Ihrem Computer zu importieren.

Container-Datei wurde nicht gefunden

Wenn beim Starten des Programms ein früher erstellter Container nicht gefunden werden kann, wird dieser Container im ViPNet SafeDisk-V-Programmfenster mit dem Symbol gezeichnet.

Wenn sich die Datei Ihres Containers auf einem Netzlaufwerk befindet und der Container sich nicht in ViPNet SafeDisk-V einbinden lässt:

- Überprüfen Sie, ob der Containername geändert wurde.
- Überprüfen Sie, ob der Pfad zur Container-Datei geändert wurde.
- Wenn sich die Datei Ihres Containers auf einem Netzlaufwerk befindet, überprüfen Sie den Status der Netzwerkverbindung.
- Wenn sich die Datei Ihres Containers auf einem Netzlaufwerk befindet, überprüfen Sie, ob sich der Name der Container-Datei geändert hat.



Achtung! Wenn Sie möchten, dass Ihr Container, der sich auf einem Netzlaufwerk befindet, als ein eigenes Netzlaufwerk freigegeben wird, dann sollte der Name der Container-Datei nicht nachträglich geändert werden.

Beim Versuch, einen nicht auffindbaren Container einzubinden, wird das Fenster **Container nicht gefunden** eingeblendet. Um den Zugang zu in diesem Container enthaltenen Daten wiederherzustellen, geben Sie den neuen Pfad zur Container-Datei an.



Abbildung 55: Container nicht gefunden

Verbindung zum Container ging verloren

Wenn zu einem Container, der sich auf einem Netzlaufwerk oder einem mobilen Datenträger befindet, keine Verbindung mehr besteht:

1. Trennen Sie den Container.
2. Richten Sie die Verbindung zum Netzlaufwerk wieder ein (oder warten Sie ab, bis die Verbindung wiederhergestellt wird).
3. Binden Sie den Container erneut ein.

Container kann nicht eingebunden werden

Wenn Sie einen Container nicht einbinden können:

- Vergewissern Sie sich, dass in der aktuellen Konfiguration von ViPNet Monitor die Verwendung von ViPNet SafeDisk-V-Containern erlaubt ist.
- Stellen Sie sicher, dass der Container nicht bereits von einem anderen Benutzer eingebunden wurde (das kann passieren, wenn Sie den Container auf ein allgemein freigegebenes Netzlaufwerk kopiert haben).

  Beachten Sie, dass zu jedem gegebenen Zeitpunkt jeweils nur ein Benutzer mit dem Container arbeiten kann.
- Stellen Sie sicher, dass für die Container-Datei das Komprimierungs- oder Verschlüsselungsattribut nicht gesetzt ist (s. Das Komprimierungs- oder das Verschlüsselungsattribut der Container-Datei ist gesetzt auf S. 130).
- Benutzen Sie die Lösung für ein verwandtes Problem (s. Container-Datei wurde nicht gefunden auf S. 128).

Das Komprimierungs- oder das Verschlüsselungsattribut der Container-Datei ist gesetzt

In der aktuellen Programmversion kann als SafeDisk-V Container keine Datei verwendet werden, bei welcher das Komprimierungs- oder das Verschlüsselungsattribut gesetzt ist. Beim Versuch, einen solchen Container einzubinden, wird eine Meldung über die Unmöglichkeit der Einbindung eingeblendet.

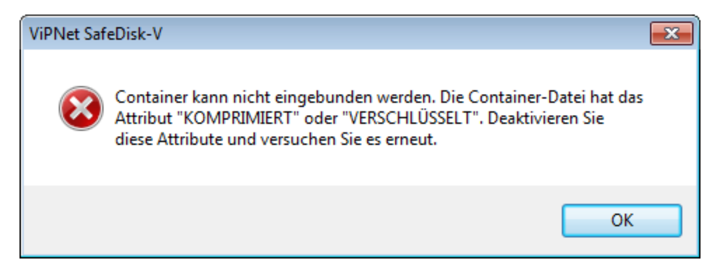
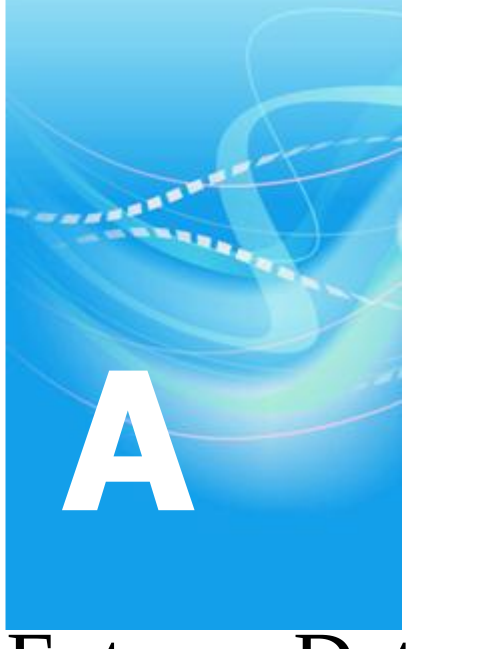


Abbildung 56: Container kann nicht eingebunden werden

Das Komprimierungs- oder Verschlüsselungsattribut kann beim Erstellen der Container-Datei automatisch gesetzt worden sein, falls das Komprimierungsattribut sowohl für das Laufwerk, auf dem der Container angelegt wird, als auch für alle untergeordneten Dateien und Ordner auf diesem Laufwerk gesetzt wurde.

Zum Zurücksetzen des Komprimierungs- oder des Verschlüsselungsattributs:

1. Klicken Sie mit der rechten Maustaste auf den Container-Dateinamen und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**.
2. Klicken Sie im Fenster der Datei-Eigenschaften in der Registerkarte **Allgemein** auf die Schaltfläche **Erweitert**.
3. Deaktivieren Sie im Fenster **Erweiterte Attribute** in Gruppe **Komprimierungs- und Verschlüsselungsattribute** die entsprechenden Kontrollkästchen.



Externe Datenträger

Allgemeine Informationen

Externe Geräte werden zum Speichern der Schlüsselcontainer verwendet. Diese Schlüsselcontainer können für die Authentifizierung, zum Erstellen von digitalen Signaturen oder für andere Zwecke verwendet werden.

Auf dem externen Gerät können Schlüssel gespeichert werden, die mit Hilfe unterschiedlicher Algorithmen in ViPNet-Software oder in Drittanwendungen erstellt wurden. Die maximale Anzahl der Schlüsselcontainer, die auf einem externen Gerät gespeichert werden können, hängt von der Speicherkapazität des Geräts ab.

Die Software ViPNet SafeDisk-V unterstützt zwei Arten der Authentifizierung mit Hilfe eines externen Geräts:

- Mit dem privaten Schlüssel des ViPNet-Benutzers, der auf dem Gerät gespeichert wird. Diese Art der Authentifizierung hat die folgenden Einschränkungen:
    - Ein externes Gerät kann nicht für die Authentifizierung mehrerer ViPNet-Benutzer verwendet werden.
    - Ein externes Gerät kann nicht für die Authentifizierung eines Benutzers auf mehreren ViPNet-Knoten verwendet werden.
    - Wenn diese Art der Authentifizierung verwendet wird, dann müssen die Signaturschlüssel des Benutzers, die mit Hilfe von ViPNet-Software in der Zertifizierungsstelle erstellt wurden, auf dem gleichen Gerät wie der private Schlüssel gespeichert sein.

- Mittels Zertifikat, das gemeinsam mit dem entsprechenden privaten Schlüssel auf dem Gerät gespeichert wird.
- Das Zertifikat für die Authentifizierung kann in der Windows-Domäne angefordert werden. Der Schlüsselcontainer wird dabei auf einem externen Gerät gespeichert, das den Standard PKCS#11 unterstützt.

Alle Operationen mit Schlüsselcontainern und externen Geräten können Sie im Programm ViPNet CSP durchführen. Damit ein externes Gerät auf dem Computer verwendet werden kann, sollten zunächst die Treiber dieses Geräts installiert werden. Stellen Sie vor dem Speichern der Schlüssel auf dem Gerät sicher, dass das Gerät formatiert ist.

Liste externer Datenträger

In der nachfolgenden Tabelle sind externe Geräte aufgelistet, die im Programm ViPNet SafeDisk-V verwendet werden können. Für jedes externe Geräte werden die Beschreibung, die Bedingungen und Besonderheit der Verwendung sowie Informationen zur Unterstützung des Standards PKCS#11 aufgeführt.



Hinweis. PKCS#11 Standard (bekannt auch als Cryptoki) gehört zur Gruppe der PKCS Standards (Public Key Cryptography Standards – Verschlüsselungsstandards für öffentliche Schlüssel), welche von der Firma RSA Laboratories entwickelt wurde. Der Standard beschreibt eine betriebssystemunabhängige API-Benutzeroberfläche für die Arbeit mit kryptografischen Authentisierungsgeräten.

Name des Geräts in Software ViPNet CSP	Vollständiger Name und Gerätetyp	Anwendungsbedingungen	Unterstützung von PKCS#11
eToken Aladdin	Persönlicher elektronischer Schlüssel **eToken PRO (Java)**, **eToken PRO** vom Hersteller Aladdin.	Auf dem Netzwerkknoten muss die Software PKI Client 5.1 oder höher installiert sein. eToken PRO SmartCard kann mit jedem PC/SC-kompatiblen Smart Card Reader benutzt werden.	Ja
iButton Aladdin	Elektronischer Schlüssel **Dallas**, **iButton** Typ **DS1993**, **DS1994**, **DS1995** und **DS1996**.	Das Lesegerät muss an den Computer angeschlossen werden. Auf dem Computer muss die Software zur Datenübertragung mit iButton, 1-Wire Drivers Version 3.20 oder Version 4.0.3 installiert sein.	Nein

Name des Geräts in Software ViPNet CSP	Vollständiger Name und Gerätetyp	Anwendungsbedingungen	Unterstützung von PKCS#11
		In den Betriebssystemen Windows XP und Server 2003 kann neben ViPNet-Software ausschließlich die Software 1-Wire Drivers Version 3.20 verwendet werden.	
Smartcard Athena	Karten mit dem Speichertyp I2C (ASE M4), synchrone Karten mit dem Bustyp 2/3 und geschütztem Speicher nach ISO7816-3 (ASE MP42).	Das Auslesen und Eintragen der Daten auf Smartcard erfolgt durch den CardReader ASEDrive III PRO-S des Herstellers Athena. Die Treiber der Version 2.6 sollen auf dem PC installiert werden.	Nein
Siemens CardOS (wird nicht von ViPNet CSP unterstützt)	SmartCards **CardOS/M4.01a,** **CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, **CardOS V4.4** vom Hersteller Atos (Siemens).	Auf dem Computer muss die Software Siemens CardOS API V5.0 oder höher installiert werden.	Ja



Regionaleinstellungen

Zur korrekten Darstellung des deutschen Interfaces von ViPNet SafeDisk-V im Betriebssystem Microsoft Windows XP/Server 2003/Vista/Windows 7/Windows 8 mit englischer Lokalisierung sollte die Unterstützungsfunktion von Umlauten und „ß“ aktiviert werden. Das gilt besonders für Programme, die keinen Unicode-Standard unterstützen. Es wird empfohlen, diese Einstellung bereits vor der Programminstallation durchzuführen.

Diese Parameter sollten auch dann eingestellt werden, wenn ein deutsches MUI (Multilanguage User Interface) installiert wurde. Das bedeutet, dass der Kern des Betriebssystems Englisch ist und die deutsche Sprache für das Interface und die Help-Dateien später installiert wurde. In diesem Fall sind die Regionaleinstellungen Englisch und sollten geändert werden.



Achtung! Zum Ändern von Regionaleinstellungen sollten Sie über Administratorrechte im Betriebssystem verfügen.

Regionaleinstellungen für Windows XP/Server 2003

So konfigurieren Sie die Spracheinstellungen für Windows XP/Server 2003:

1 Wählen Sie **Systemsteuerung** (**Control Panel**) im Menü **Start** aus.

2 Klicken Sie auf **Regions- und Sprachoptionen** (**Regional and Language Options**).

3 Gehen Sie zu der Registerkarte **Erweitert** (**Advanced**) im Fenster **Regions- und Sprachoptionen** (**Regional and Language Options**)

4 Wählen Sie **Deutsch** (**German**) aus.

5 Aktivieren Sie das Kontrollkästchen **Alle Einstellungen auf das Benutzerkonto und Standardbenutzerprofil anwenden** (**Apply all settings to the current user account and to the default user profile**).

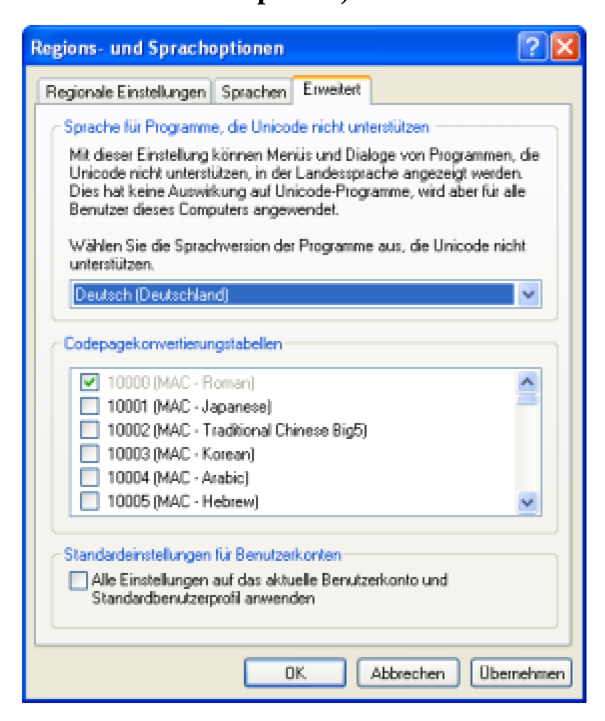


Abbildung 57: Sprachauswahl für Programme, die Umlaute und „ß“ nicht unterstützen

6 Klicken Sie auf **OK**. Möglicherweise muss der Computer neu gestartet werden.

Regionaleinstellungen für Windows Vista/Server 2008/Windows 7

Auf diese Weise erreichen Sie die korrekte Darstellung der Umlaute und „ß“ für Windows Vista/Server 2008/Windows 7:

1 Wählen Sie Systemsteuerung im Menü **Start** > **Systemsteuerung** (**Control Panel**) > **Zeit, Sprache und Region** (**Clock, Language, and Region**) > **Region und Sprache** (**Region and Language**) aus.

2 Klicken Sie auf die Registerkarte **Verwaltung** (**Administrative**) im Fenster **Region und Sprache** (**Region and Language**).

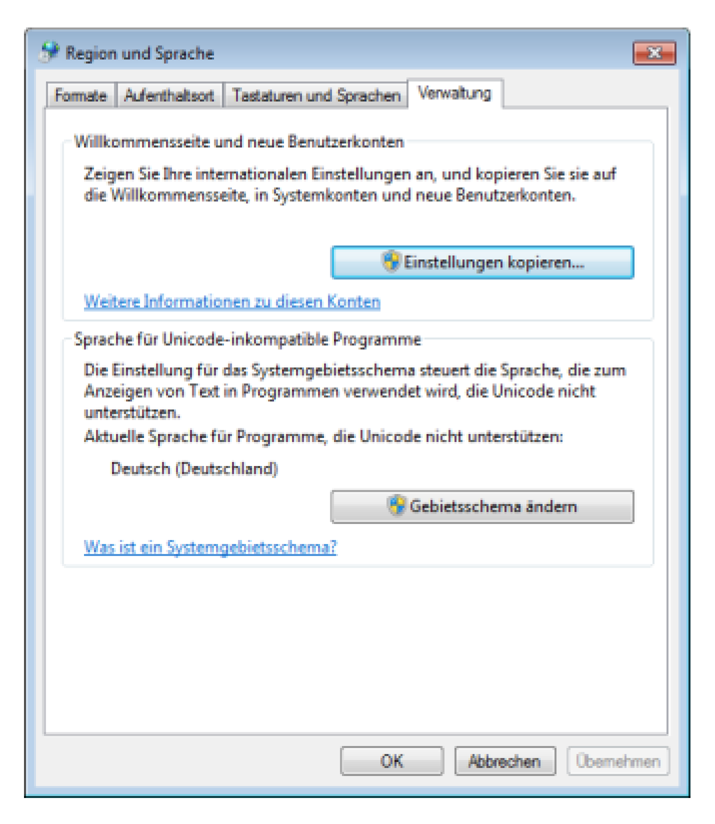


Abbildung 58: Erweiterte Spracheinstellungen

3 Klicken Sie auf **Gebietsschema ändern** (**Change system locale**) in der Registerkarte **Verwaltung** (**Administrative**).

4 Wählen Sie **Deutsch (Deutschland)** im neu geöffneten Fenster in der Liste **Aktuelles Gebietsschema** aus und klicken auf **OK**.

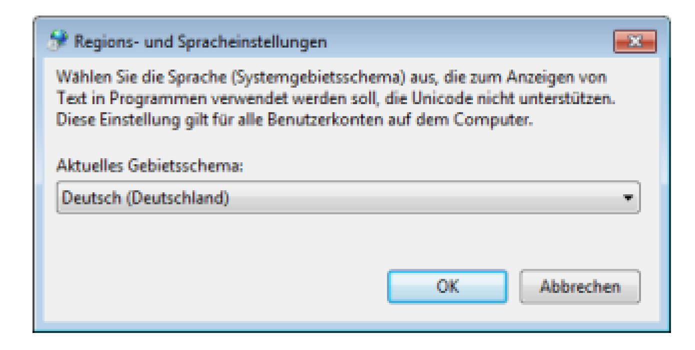


Abbildung 59: Auswahl der Systemsprache

5 Klicken Sie auf **OK**. Der Computer muss neu gestartet werden.

6 Nach dem Neustart öffnen Sie **Systemsteuerung** (**Control Panel**) > **Zeit, Sprache und Region** (**Clock, Language, and Region**) > **Region und Sprache** (**Region and Language**).

7 Klicken Sie auf die Registerkarte **Verwaltung** (**Administrative**) im Fenster **Region und Sprache** (**Region and Language**).

8 Klicken Sie auf die Schaltfläche **Einstellungen kopieren** (**Copy settings**) in der Registerkarte **Verwaltung** (**Administrative**).

9 Aktivieren Sie das Kontrollkästchen **Willkommensseite und Benutzerkonten** (**Welcome screen and system accounts**) im neu geöffneten Fenster und klicken auf **OK**.

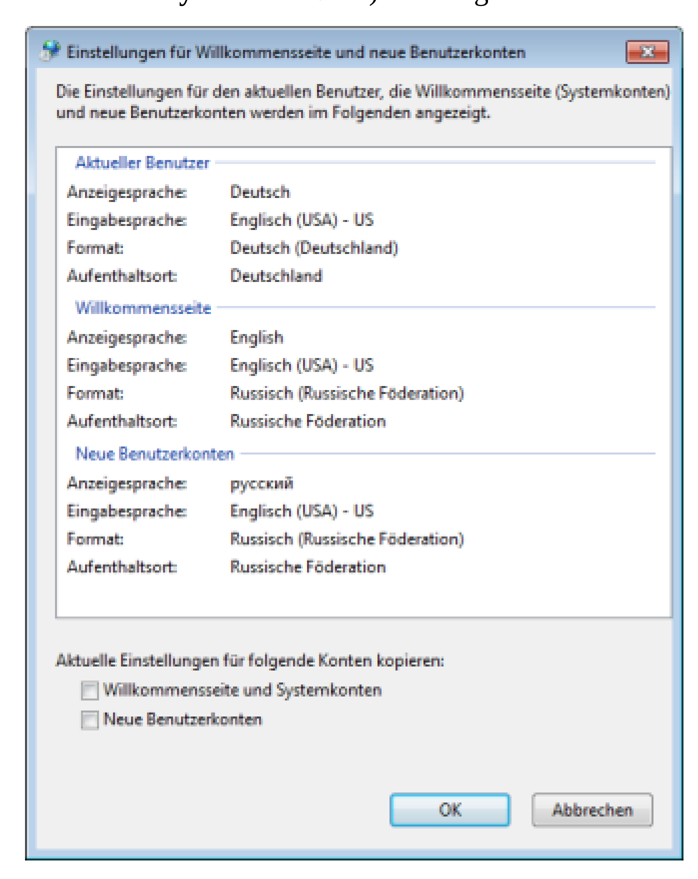


Abbildung 60: Kopieren der Parameter

Um weitere Probleme mit der Zeichencodierung auf einigen Systemen zu vermeiden, nehmen Sie die folgenden Einstellungen vor:

1 Gehen Sie zur Registerkarte **Formate** (**Formats**) des Fensters **Region und Sprache** (**Region and Language**) und wählen Sie **Deutsch (Deutschland)** in der Liste **Format** aus.

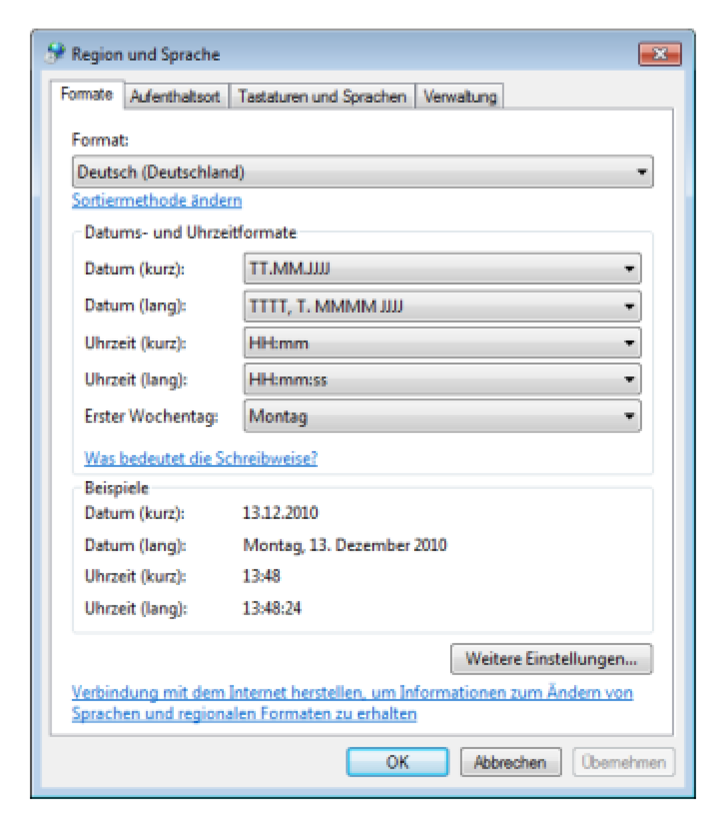


Abbildung 61: Einstellung von Formaten

2 Gehen Sie zur Registerkarte **Aufenthaltsort** (**Location**) des Fensters **Region und Sprache** (**Region and Language**) und wählen Sie **Deutschland** in der Liste **Aktueller Aufenthaltsort** (**Current location**) aus.

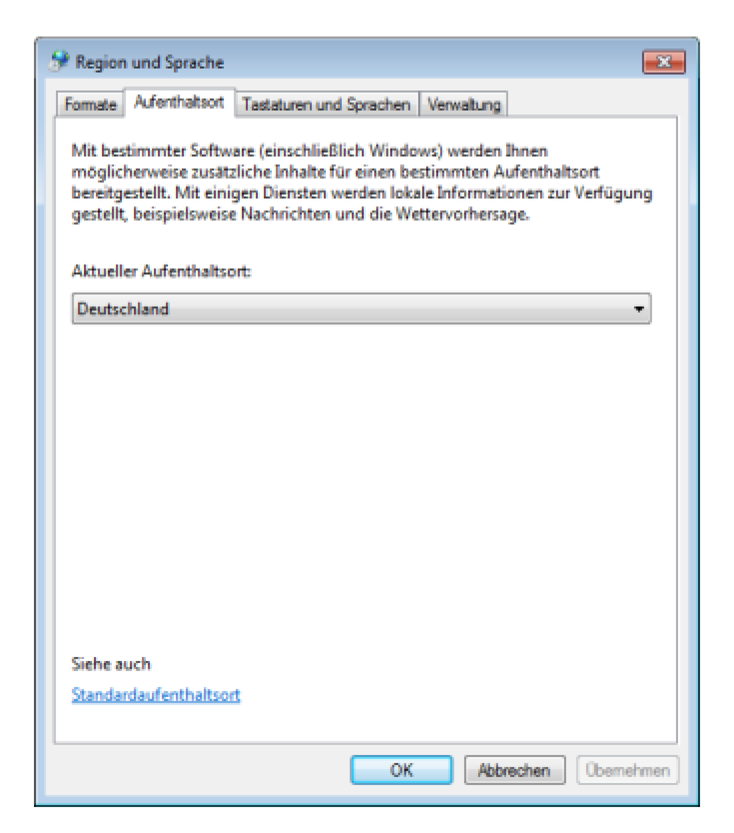


Abbildung 62: Auswahl des aktuellen Aufenthaltsortes



Versionsgeschichte

In dieser Anwendung werden die wichtigsten Änderungen in den vorherigen Versionen von ViPNet SafeDisk-V beschrieben.

Neu in Version 4.1.1

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten von ViPNet SafeDisk-V der Version 4.1.1 geboten.

- **Zugriffssteuerung auf SafeDisk-V Container**

  Es besteht die Möglichkeit zur Steuerung des Zugangs zu geschützten Containern von SafeDisk-V in Abhängigkeit zur jeweiligen Konfiguration des Programms ViPNet Monitor. Beim Wechsel zu einer Konfiguration, in der die Verwendung von SafeDisk-V-Containern nicht erlaubt ist, werden alle eingebundenen Container getrennt. Beim Wechsel zu einer Konfiguration, in der die automatische Einbindung von Containern erlaubt ist, werden alle Container, für welche die entsprechende Option eingestellt wurde, automatisch eingebunden.

Neu in Version 4.0.2

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten von ViPNet SafeDisk-V der Version 4.0.2 geboten.

- **Zwangsweise Trennung des Containers**

  Es besteht die Möglichkeit zur zwangsweisen Trennung des Containers, wenn die im Container enthaltenen Dateien von anderen Anwendungen benutzt werden.

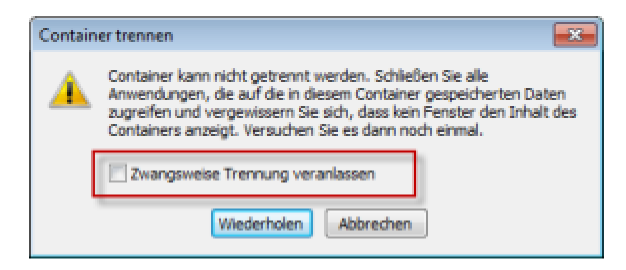


Abbildung 63: Zwangsweise Trennung des Containers

- **Formatierung des Containers**

  Zum Formatieren des Containers wurde früher die Standardschnittstelle von Microsoft Windows verwendet. Aus praktischen Gründen wurde dafür nun ein Assistent zur Containerformatierung implementiert. Der Assistent zur Containerformatierung wird beim Einbinden eines nicht formatierten Containers automatisch gestartet.



Abbildung 64: Eine Möglichkeit den Container mit Hilfe des Assistenten zu formatierem

Neu in Version 4.0.1

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten von ViPNet SafeDisk-V der Version 4.0.1 geboten.

- **Die Integration von Software ViPNet SafeDisk-V mit ViPNet Client**

  Dank der Integration wird ein zusätzlicher Schutz vertraulicher Daten, die in den Containern von ViPNet SafeDisk-V (auf S. 146) gespeichert sind, gewährleistet. Nun wird der Containerzugang im Programm ViPNet SafeDisk-V durch die aktuelle Konfiguration von ViPNet Monitor (geschützt oder ungeschützt) gesteuert.

Neu in Version 4.0

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten von ViPNet SafeDisk-V der Version 4.0 geboten.

- **Austausch von Containerschlüsseln**

  Damit die Sicherheit beim Schutz von Daten, die in SafeDisk-V Containern gespeichert sind, erhöht werden kann, besteht die Möglichkeit zum Aktualisieren der Containerschlüssel, mit denen der Containerinhalt verschlüsselt wurde. Nach der Aktualisierung wird der Zugang zum Container unter Verwendung alter Schlüssel nicht mehr möglich sein. Es wird empfohlen, die Aktualisierung der Containerschlüssel nicht seltener als alle 15 Monate durchzuführen.

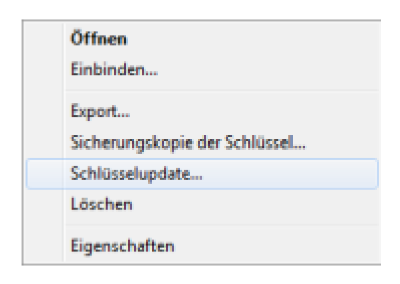
  

  Abbildung 65: Containerschlüsselupdate

- **Speicherung der Sicherungskopie der Containerschlüssel auf einem externen Gerät**

  Damit die Sicherheit beim Schutz von Daten, die in SafeDisk-V Containern gespeichert sind, erhöht werden kann, besteht nun die Möglichkeit zum Speichern von Sicherungskopien der Containerschlüssel auf einem externen Gerät (Authentisierungsgerät). Details s. Liste unterstützter Geräte (s. Externe Datenträger auf S. 131).



Glossar

C

Client

Netzwerkknoten, der entweder einen Ausgangs- oder Endpunkt für die Datenübertragung darstellt. Im Vergleich mit dem Coordinator verfügt der Client über keine Routing-Funktionen.

Siehe: Coordinator (ViPNet Coordinator) (auf S. 143), Routing, ViPNet Netzwerkknoten (auf S. 146).

Container

Siehe Container-Datei (auf S. 143).

Container-Datei

Eine Datei, welche die geschützten Daten beinhaltet. Diese Datei wird als ein Laufwerk unter Windows angezeigt. Sie können mit ihr wie mit einem Laufwerk arbeiten und dort Dateien speichern, kopieren, einfügen, verschieben, löschen usw.

Eine Containerdatei hat die Dateierweiterung *.sdc und ist standardmäßig ausgeblendet. Um diese Datei anzusehen wählen Sie in der Windows-Explorer Menüleiste unter **Extras** den Menüpunkt **Ordner- und Suchoptionen** und auf der Registerkarte **Ansicht** deaktivieren Sie die Option **Geschützte Dateien ausblenden (empfohlen)**.

Coordinator (ViPNet Coordinator)

Netzwerkknoten mit installierter ViPNet Coordinator Software.

Siehe: Routing, ViPNet Netzwerk.

E

Exportdatei des Containers

Diese Datei wird beim Containerexport erstellt. Sie beinhaltet die exportierte Containerdatei und die Sicherungskopie der Containerschlüssel.

Sie können einen Container exportieren, wenn Sie eine vollständige Sicherungskopie aller Daten erstellen wollen, die im Container enthalten sind, oder wenn Sie einem anderen Benutzer den Zugriff auf die geschützten Daten ermöglichen wollen.

Die Exportdatei des Containers hat die Erweiterung `*.sdx`.

Siehe: Sicherungskopie der Containerschlüssel (auf S. 145).

K

Key Center (KC)

Eine der Software-Komponenten von ViPNet Administrator.

Siehe: Key Center Administrator, Stammzertifikat, ViPNet Benutzer, ViPNet Administrator.

M

Modus „Extreme Gefahr“

Spezialmodus von ViPNet Safe Disk, der es ermöglicht, alle Daten in den Containern unverzüglich zu löschen, wenn beim Näherkommen unberechtigter Übeltäter keine andere Wahl mehr bleibt.

Siehe: Modus „Gefahr“ (auf S. 144).

Modus „Gefahr“

In diesem Modus können alle Container sofort getrennt werden.

Siehe auch: Modus „Extreme Gefahr“ (auf S. 144).

N

Network Control Center (NCC)

Eine der Software-Komponenten von ViPNet Administrator.

Siehe: Adresslisten, Benutzerrechte, Netzwerkobjekt, Key Center (KC) (auf S. 144), ViPNet Administrator.

R

Rolle

Die Rolle bestimmt die angewandte Funktionalität der ViPNet Software auf einem bestimmten Netzwerkknoten und wird in der Lizenz-Datei infotecs.reg gespeichert. Eine ViPNet Anwendung kann mehrere Rollen tragen, jede Rolle hat ihren eigenen Namen.

Siehe: Benutzerrechte, ViPNet Netzwerk.

S

Schlüsseldistribution

Die Datei mit der Erweiterung .dst, wird im ViPNet Network Manager oder NCC erstellt. Die Datei beinhaltet Schlüsselinformationen, Adresslisten und die Lizenzdatei, die für den initialen Start des Netzwerkknotens erforderlich sind.

Siehe: Adresslisten, ViPNet Netzwerkknoten (auf S. 146), Key Center (KC) (auf S. 144), Lizenzdatei.

Sicherungskopie der Containerschlüssel

Spezielle Datei, die eine Kopie der Schlüssel enthält, mit deren Hilfe der Container geschützt wird. Wenn die Schlüssel-Datei für den Zugang zum Container beschädigt ist, oder Sie aus anderen Gründen den Zugang zum Container nicht erhalten, verwenden Sie zum Wiederherstellen des Containerzugangs die Sicherungskopie der Containerschlüssel. Sie können die Sicherungskopie auch verwenden, um jemand anderem Zugang auf Ihren Container zu gewähren.

Die Datei mit der Sicherungskopie der Containerschlüssel hat die Erweiterung `*.sde`.

V

ViPNet Network Manager

Verwaltungsmodul aus dem Paket ViPNet VPN, dient zum Erstellen und Verwalten kleiner und mittlerer ViPNet Netzwerke.

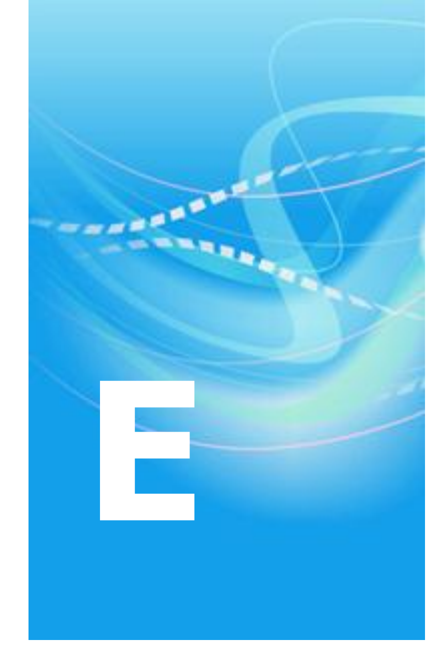
ViPNet Netzwerkknoten

Rechner mit installierter ViPNet Software.

Siehe: ViPNet Netzwerk, Digitale Signatur.

ViPNet SafeDisk-V

Die Software ViPNet Safe Disk-V ist ein Bestandteil der Softwarelösung ViPNet VPN. ViPNet Safe Disk-V ist dafür bestimmt, vertrauliche Daten zu schützen. Zum Speichern vertraulicher Daten wird im Programm ViPNet Safe Disk-V ein Container erstellt, der eine verschlüsselte Datei auf der Festplatte oder auf einem mobilen Datenträger darstellt.



Index